НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
Факультет інформатики та обчислювальної техніки
Кафедра автоматики та управління в технічних системах

«До захисту допущено»
Завідувач кафедри
_____ Ролік О.І.
(підпис) (ініціали, прізвище)
“___”_____2019

Дипломний проект

освітньо-кваліфікаційного рівня «бакалавр»

зі спеціальності 6.050201 «Системна інженерія»
(код і назва)

на тему: Захищена корпоративна мережа на базі технології MPLS

Виконав: Русило Юліан Миколайович _____
(підпис)

Керівник: Дорогий Я.Ю. _____
(підпис)

Рецензент доцент кафедри ТК, к.т.н. Ткач М. М. _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2019 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО”

Факультет інформатики та обчислювальної техніки
Кафедра автоматики та управління в технічних системах
Ступінь вищої освіти перший (бакалаврський)
Спеціальність 6.050201 «Системна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____О.І.Ролік
(підпис) (ініціали, прізвище)
“__”_____2019 р.

ЗАВДАННЯ

на дипломний проект освітньо-кваліфікаційного рівня "бакалавр"

Студенту Русилу Юліану Миколайовичу
(прізвище, ім’я, по батькові)

1. Тема проекту Захищена корпоративна мережа на базі технології MPLS
керівник проекту Дорогий Ярослав Юрійович, к.т.н., доц. _____,

затверджені наказом по університету від «__» _____ 2019 р. №_____
2. Термін подання студентом проекту «__» _____ 2019 р.
3. Вихідні дані до проекту _____
_____
_____
4. Перелік питань, які мають бути розроблені:
_____
_____
_____
_____

5. Перелік графічного матеріалу:

6. Консультанти розділів проекту:

з технічної частини _____к.т.н. доцент Дорогий Я.Ю._____

7. Дата видачі завдання “___” _____2019_р.

Керівник дипломного проекту _____Я.Ю.Дорогий_____
(підпис)

Завдання прийняв до виконання _____Ю.М.Русило_____
(підпис)

ЗАТВЕРДЖУЮ
Керівник дипломного проекту
_____ Я.Ю.Дорогий
(підпис) (ініціали, прізвище)
“__.__.” _____2019_р.

КАЛЕНДАРНИЙ ПЛАН-ГРАФІК

виконання дипломного проекту

студентом Русилом Юліаном Миколайовичем
(прізвище, ім'я, по батькові)

№ з/п	Назва етапів виконання дипломного проекту	Термін виконання	Примітка
1			
2			
3			
4			
4			
5	Оформлення текстової та графічної документації	20.05.2019	
6	Подання проекту до попереднього захисту	04.06.2019	
7	Представлення до захисту		

Студент _____ Ю.М.Русило
(підпис) (ініціали, прізвище)
Керівник проекту _____ Я.Ю.Дорогий
(підпис) (ініціали, прізвище)

АНОТАЦІЯ

Русило Ю.М. Захищена корпоративна мережа на базі технології MPLS. НТУУ «КПІ ім. Ігоря Сікорського», Київ, 2019.

У даному дипломному проекту наведено огляд підходів до побудови корпоративної мережі. Проведено аналіз існуючого обладнання та обґрунтований вибір для реалізації проекту. У якості демонстраційної частини розроблено модель корпоративної мережі на базі протокола MPLS, виконані потрібні налаштування та перевірена її працездатність.

Проект містить 62 с. тексту, 18 рисунків, 1 таблицю, 16 літературних джерел.

Ключові слова: корпоративна мережа, BGP, MPLS, Dynamips, GNS3.

Annotation

Rusilo Yu.M. Secured corporate network based on MPLS technology. NTUU "Igor Sikorsky Kyiv Politechnic Institute", Kyiv, 2019.

This graduation project gives an overview of approaches to building a corporate network. An analysis of the existing equipment and a reasonable choice for the project implementation have been carried out. As a demonstration part, a corporate network model based on the MPLS protocol was developed, the necessary settings were made and its performance tested.

The work contains 62 p. of text, 18 pictures, 1 table, 16 references.

Keywords: corporate network, BGP, MPLS, Dynamips, GNS3.

ЗМІСТ

Сторінка

ВСТУП

Актуальність роботи. Сучасна епоха характеризується стрімким процесом інформатизації суспільства. Найсильніше це проявляється у зростанні пропускної здатності та гнучкості інформаційних мереж. Смуга пропускання в розрахунку на одного користувача стрімко збільшується завдяки кільком чинникам. По-перше, зростає популярність застосувань World Wide Web і кількість електронних банків інформації, які стають надбанням кожної людини. Падіння цін на комп'ютери призводить до зростання числа персональних комп’ютерів, кожен з яких потенційно перетворюється на пристрій, здатний підключитися до мережі Internet. По-друге, нові мережеві застосування стають більш вимогливими щодо смуги пропускання - входять в практику програми Internet, орієнтовані на мультимедіа і відеоконференцзв'язок, коли одночасно відкривається дуже велика кількість сесій передачі даних. Як результат, спостерігається різке зростання в споживанні ресурсів Internet - за оцінками середній обсяг потоку інформації в розрахунку на одного користувача у світі збільшується в 8 разів щороку.

Об’єкт дослідження – методи побудови захищеної корпоративної мережі.

Предметом дослідження в роботі є побудова захищеної корпоративної мережі на базі технології MPLS.

Зв’язок роботи з науковими програмами, планами, темами. Тематика роботи включена в науково-технічні плани кафедри автоматики та управління в технічних системах Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Метою даного проекту є розробка моделі та впровадження захищеної інформаційно-обчислювальної мережі корпоративного масштабу. Побудована мережа має відповідати наступним вимогам:

– масштабованість;

– відмовостійкість;

– швидка конвергенція;

– висока пропускна здатність;

– балансування навантаженням.

Розроблена мережа повинна задовольняти потреби великого підприємства, який складається з декількох віддалених відділень. А саме, забезпечити швидку передачу даних між її відділеннями з дотриманням високих вимог щодо забезпечення конфіденційності та захищеності обмінюваних даних. Також треба забезпечити можливість ефективного масштабування розміру мережі як в сторону збільшення кількості мережевого обладнання, так і в сторону його зменшення.

Для досягнення поставленої мети потрібно розв’язати наступні задачі, необхідні для побудови нашої мережі:

– аналіз технологій побудови корпоративних мереж;

– вибір виробника обладнання та необхідного обладнання;

– проектування та моделювання створеної мережі.

Методи дослідження, використані в роботі: теоретичний аналіз, системний підхід, експеримент та порівняння.

Практична цінність дослідження полягає у розробці оптимальної, з точки зору ефективності, зручності, швидкодії та якості моделі мережі, яка у перспективі може бути поширена серед широкої маси споживачів.

1 ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

1.1 Маршрутизуючі протоколи

Маршрутизуючий протокол – це протокол, що визначає таких формат заголовків пакетів, який надає достатньо інформації для маршрутизації пакетів. Далі будуть розглянуті найбільш використовувані та перспективні маршрутизуючі протоколи.

1.1.1 Internet Protocol version 4

Інтернет-протокол (IP) є основним протоколом зв'язку, що використовується для ретрансляції дейтаграм (пакетів) всередені мережі там у міжмережому середовищі. Відповідальний за маршрутизацію пакетів через кордони мереж, це основний протокол, на якому базується Інтернет.

Протокол IP має своїм завданням доставку дейтаграм від хоста відправника до хосту призначення виключно на основі їх адрес. Для цього, протокол IP визначає методи і структури для інкапсуляції дейтаграм.

Історично склалося, що IP представляв собою службу передачі датаграм без підтримки з’єднань в оригінальній програмі Control Transmission, розробленій Вінтом Серфом і Бобом Каном в 1974 році. В цій програмі було також використано орієнтований на з'єднання протокол управління передачею (TCP). Тому Internet Protocol Suite часто називають стеком TCP / IP.

Перша поширена версія IP, яка отримала назву Інтернет-протокол версії 4 (IPv4) є домінуючим протоколом в Інтернеті, хоча наступник, Інтернет-протокол версії 6 (IPv6) знаходиться в активній фазі розвитку та впровадження провайдерами доступу до Інтернет по всьому світу.

Інтернет-протокол відповідає за адресування вузлів та маршрутизацію дейтаграм (пакетів) від хоста відправника до хосту призначення через одну або кілька IP-мереж. Для цієї мети Інтернет-протокол визначає систему адресації, яка має дві функції. Адреси однозначно ідентифікують хости та забезпечують можливість логічного пошуку їх місцезнаходження. До кожного пакету додається заголовок, що містить мета-дані для доставки. Цей процес позначення пакетів також називається інкапсуляцією.

Принципи побудови інтернет-протоколів припускають, що мережева інфраструктура є ненадійною в будь-якій окремій частині мережі або середовища передачі, і що він динамічний з точки зору наявності зв'язків та вузлів. Не існує централізованого моніторингу чи засобу вимірювання продуктивності, який би відстежував стан мережі. В інтересах зниження складності мережі, прийняття рішень в мережі навмисно головним чином розташовані в кінцевих вузлах кожної передачі даних, що отримало назву принцип «з кінця в кінець». Маршрутизатори на шляху передачі просто пересилають пакети до наступного відомого шлюзу, який відповідає префіксу маршрутизації для адреси призначення.

Як наслідок цього дизайну, інтернет-протокол не надає засобів перевірки, контролю та гарантування доставки пакетів. Цей протокол не встановлює з’єднання при передачі даних, на відміну від так званих орієнтованих на з'єднання режимів передачі. Відсутність надійності може викликати наступні ситуації:

- пошкодження даних;
- втрачених пакетів даних;
- дублікат прибуття;
- порушення послідовності доставки пакетів.

Так як маршрутизація є динамічною, а також шлях проходження пакету не зберігається, не виключено, що перший пакет має довший шлях до місця призначення ніж послідуючі датаграми.

Єдиним механізм перевірки пакетів, який надає інтернет-протокол версії 4 (IPv4), є перевірка IP-заголовку на наявність пошкоджених даних шляхом передачі разом з пакетом його контрольної суми. Якщо при перевірці на проміжному або кінцевому пункті передачі виявляється наявність помилки, пакет відкидається.

В IPv6, з іншого боку, відмовилася від використання IP-заголовку контрольні суми на користь швидкої переадресації через елементи маршрутизації в мережі.

Рішення або виправлення будь-яких з цих проблем надійності є відповідальністю протоколу верхнього рівня. Наприклад, щоб забезпечити доставку пакетів у правильному порядку, прокол верхнього рівня має зберігати отримані дані до моменту, коли вони будуть передані програмі.

На додаток до питань надійності, динамічний характер і різноманітність Інтернету та його компонентів не дають ніяких гарантій, що той чи інший шлях насправді підходить для виконання передачі даних, навіть якщо шлях є доступним і надійним. Один з технічних обмежень є розмір пакетів даних, що допускається передавати через вказаний канал зв’язку. Додаток повинен гарантувати, що він використовує належні характеристики передачі. Існують послуги для автоматичного визначення максимального блоку передачі (MTU) локальної зв'язку, а також протягом усього прогнозованого шляху до місця призначення при використанні IPv6. IPv4 має можливість автоматичного фрагментування вихідної дейтаграми на більш дрібні одиниці для передачі. У цьому випадку IP надає механізми для визначення правильного порядку фрагментів для відтворення повідомлення на стороні призначення.

Мабуть, найбільш складним аспектом IP є адресація і маршрутизація. Адресація визначає як кінцевим вузлам призначаються IP-адреси і як підмережі IP-адрес розділяються і групуються разом. IP-маршрутизація виконується на всі точках шляху передачі пакету, але найголовніше на міжмережевих маршрутизаторах, які зазвичай використовують або внутрішні протоколи

маршрутизації (IGP) або зовнішні (EGPs) для забезпечення необхідною інформацією для пересилки пакетів в інші IP-мережі.

1.1.2 Internet Protocol version 6

Наприкінці 1980-х стала очевидною нестача адресного простору Інтернет. На початку 1990-х, навіть після введення безкласової адресації, виявилось, що однієї економії та використання NAT'у буде замало для попередження вичерпання адресного простору, і необхідна зміна адресації. Крім того, накопичилась певна кількість пропозицій щодо усунення недоліків існуючої моделі Інтернет. Наприкінці 1992 року IETF оголосила конкурс на створення протоколу Інтернет наступного покоління (англ. IP Next Generation — IPng). 25 липня 1994 року IETF ствердила модель IPng з утворенням кількох робочих груп IPng. У 1996 булу створено серію RFC, що визначали новий протокол Інтернет. Оскільки версія 5 вже була раніше призначена експериментальному протоколу передачі мультимедійних потоків, новий протокол отримав версію 6.

Оцінки повного вичерпання IPv4 адрес розрізнялись в 2000-х, але на даний момент можна сказати, що цей вже сталося. В 2003 році директор APNIC Пол Уілсон (англ. Paul Wilson) заявив, що, виходячи з темпів поширення мережі Інтернет того часу, вільного адресного простору вистачить на одно-два десятиріччя. В вересні 2005 року Cisco Systems відмітила, що пула доступних адрес вистачить на 4 — 5 років. У вересні 2010, виходячи з даних IANA, весь пул адрес IPv4 буде виділений реєстратурам (RIR)) до середини 2011 року ([2]), в листопаді ця дата була перенесена на березень 2011. 3 лютого 2011 року IANA виділила останні п’ять блоків IP-адрес /8 (IPv4).

Розширення адресного простору скасовує необхідність використання NAT, оскільки на кожну людину припадає близько 3*108 унікальних адрес. Принцип призначення хосту IPv6 адреси є ієрархічним. Мінімальний розмір підмережі - /64 (264). Молодша частина адреси (64 біти) використовується як унікальний ідентифікатор користувача, наступна частина визначає підмережу

всередині оператора зв'язку, далі йде ідентифікатор самого оператора. Такий підхід значно спрощує маршрутизацію.

З IPv6 видалено кілька функцій, що ускладнюють роботу маршрутизаторів:

Маршрутизатори більше не розбивають (фрагментують) пакет на частини (розбиття пакета можливо тільки на боці передавача). Відповідно, оптимальний MTU має визначатися за допомогою Path MTU discovery. Для покращення роботи протоколів, що потребують низького рівня втрати пакетів, мінімальний MTU збільшений до 1280 байт. Інформація про фрагментацію пакетів перенесена з основного заголовку в розширені;

Зникла контрольна сума. Оскільки канальні (Ethernet) та транспортні (TCP) протоколи також перевіряють коректність пакета, контрольна сума на рівні IP вважається зайвою. Крім того, кожен маршрутизатор зменшує hop limit на одиницю, що призводить до потреби у перерахуванні суми в IPv4.

Незважаючи на суттєве збільшення розміру адреси IPv6, завдяки цим покращенням основний заголовок пакета збільшився лише у 2 рази: з 20 до 40 байт. Покращення IPv6 у порівнянні з IPv4:

– В надшвидкосних мережах можлива підтримка надвеликих пакетів (джамбограм) — до 4 гігабайт;

– Time to Live перейменовано в Hop limit;

– З'явились відмітки потоків та класи трафіка;

– З'явилась багатоадресна передача;

– Протокол IPsec з рекомендованого перетворився на обов'язковий.

У момент ініціалізації мережевого інтерфейсу йому призначується локальна IPv6-адреса, з префіксом fe80::/10, у молодшій частині адреси розміщується ідентифікатор інтерфейсу. У якості ідентифікатора інтерфейсу часто використовується 64-бітний розширений унікальний ідентифікатор EUI-64, що найчастіше формується з MAC-адреси. Локальна адреса дійсна тільки в межах мережевого сегменту канального рівня, і використовується, в основному, для обміну інформаційними ICMPv6 пакетами.

Для отримання інших адрес вузол може запросити інформацію про налаштування мережі у маршрутизаторів за допомогою ICMPv6 повідомлення «Router Solicitation». Цей запит відсилається на групову (multicast) адресу маршрутизаторів. У відповідь маршрутизатори відсилають ICMPv6 повідомлення «Router Advertisement», що може містити інформацію про префікс мережі, адресу шлюзу, адреси рекурсивних DNS серверів [3], MTU та багато інших параметрів. Поєднуючи мережевий префікс та ідентифікатор інтерфейсу, вузол отримує нову адресу. Для захисту персональних даних ідентифікатор інтерфейсу може бути замінений на псевдовипадкове число.

Для більшого адміністративного контролю може бути використаний DHCPv6, що дозволяє адміністратору маршрутизатора призначати вузлам конкретні адреси.

Введення поля «Відмітка потоку» в протоколі IPv6 дозволяє значно спростити процедуру маршрутизації однорідного потоку пакетів. Потік — це послідовність пакетів, що надсилаються відправником певному адресату. При цьому припускається, що всі пакети даного потоку мають бути оброблені певним чином. Характер даної обробки задається додатковими заголовками.

Припускається існування декількох потоків між відправником та отримувачем. Відмітка потоку призначається вузлом-відправником шляхом генерації псевдовипадкового 20-бітного числа. Всі пакети одного потоку мають містити однакові заголовки, що оброблюються маршрутизатором.

При отриманні першого пакету з відміткою потока маршрутизатор аналізує додаткові заголовки, виконує певні операції відповідно до цих заголовків та запам'ятовує результати обробки (адресу наступного вузла, опції заголовку переходів, переміщення адрес у заголовку маршрутизації та ін.) в локальному кеші. Ключем для такого запису є комбінація адреси відправника та відмітки потоку. Наступні пакети з тією самою комбінацією адреси відправника та відмітки потоку обробляються з урахуванням інформації кеша без детального аналізу усіх полів заголовка.

Час життя запису у кеші становить не більше 6 секунд, навіть якщо пакети цього потоку продовжують поступати. Після видалення запису з кеша при отриманні наступного пакета потоку, пакет обробляється у звичайному режимі і для нього відбувається формування нового запису в кеші. Слід зауважити, що вказаний час життя потоку може бути явно заданий вузлом відправником за допомогою протоколу керування або опцій заголовку переходів, і може перевищувати 6 секунд.

Пріоритезація пакетів забезпечується маршрутизаторами на основі перших шести біт поля Traffic Class. Перші три біти визначають клас трафіка, решта бітів визначають пріоритет видалення. Чим більше значення пріоритету, тим вище пріоритет пакета.

В залежності від задач розробники IPv6 рекомендують використовувати наступні коди класу трафіку (таблиця 1.1).

Таблиця 1.1 – Класи трафіку QoS

Клас трафіку	Призначення
0	Нехарактеризований трафік
1	Заповнюючий трафік (мережеві новини)
2	Несуттєвий інформаційний трафік (електрона пошта)
3	Резерв
4	Суттєвий трафік (FTP, HTTP, NFS)
5	Резерв
6	Інтерактивний трафік (Telnet, X-terminal, SSH)
7	Керуючий трафік (Маршрутна інформація, SNMP)

1.2 Технології розподілених мереж

1.2.1 Frame Relay

Frame Relay є стандартизованою технологією WAN-мереж, яка визначає фізичний і логічний шар цифрових каналів телекомунікацій з використанням методології пакетної комутацією. Спочатку розроблений для транспорту через

Integrated Services Digital Network (ISDN) інфраструктура, він може бути використаний сьогодні в контексті багатьох інших мережевих інтерфейсів.

Провайдери доступо до Інтернет зазвичай використовують Frame Relay для передачі голосу (VoFR) і даних в якості технології інкапсуляції другого рівня по моделі OSI, що використовується між локальним мережам (LAN) через глобальну мережу (WAN). Кожен кінцевий користувач отримує приватні (виділені) лінії до комутатора Frame Relay. Мережа Frame Relay виконує передачу даних по часто часто-змінюваним шляхам абсолютно прозоро для кінцевих користувачів.

Frame Relay став одним з найбільш широко використовуваних протоколів WAN. Його дешевизна (порівняно з виділеним лініям) стала однією з причин його популярності. Крайня простота налаштування абонентського обладнання в мережі Frame Relay являє собою ще одну з причин популярності Frame Relay.

З появою технології Ethernet по оптичному каналу, технологій MPLS, VPN і розповсюдженню виділених широкополосних послуг, таких як кабельні модеми та DSL, технологія Frame Relay почала втрачати популярність. Наразі цей протокол здебільшого використовується у віддалених місцевостях по причині відсутності можливості використання зазначених вище технологій.

Frame Relay, більше спрямований на ефективне використання наявних матеріальних ресурсів, які дозволяють запропонувати послуги передачі даних, телекомунікаційними компаніями (телекомунікаційні компанії) для своїх клієнтів, а клієнти навряд чи буде використовувати послугу передачі даних 100 відсотків часу. В останні роки, Frame Relay придбав погану репутацію на деяких ринках через надмірне надлишкове бронювання пропускної здатності телекомунікаційними компаніями.

Телекомунікаційні компанії часто продають частину пропускної здатності каналу іншим підприємствам, шукають дешеву альтернативу виділеним лініям; його використання в різних географічних районах в значній мірі залежить від політики урядових і телекомунікаційних компаній.

AT & T в даний час є найбільшим власником послуг на базі технології Frame Relay у Сполучених Штатах, з локальними мережами в 22 штатах, а також національні і міжнародні мережі. Це число зміниться, коли термін дії більшість існуючих закінчиться. Багато клієнтів, швидше за все, перейдуть на технології MPLS over IP через Ethernet протягом найближчих двох років, що в багатьох випадках дозволить знизити витрати і підвищити керованість і продуктивність своїх глобальних мереж.

1.2.2 Asynchronous Transfer Mode

ATM являє собою мережеву високопродуктивну технологію комутації та мультиплексування, заснована на передачі даних у вигляді осередків (cell) фіксованого розміру (53 байти), з яких 5 байтів використовується під заголовок. На відміну від синхронного способу передачі даних (STM), ATM краще пристосований для надання послуг передачі даних з сильно розрізняються чи змінюваним бітрейтом.

Кореневі технології ATM були розроблені незалежно у Франції і США в 1970-х двома вченими: Jean-Pierre Coudreuse, який працював у дослідницькій лабораторії France Telecom, і Sandy Fraser, інженер Bell Labs. Вони обидва хотіли створити таку архітектуру, яка б здійснювала транспортування як даних, так і голосу на високих швидкостях, і використовувала мережеві ресурси найбільш ефективно.

Комп'ютерні технології створили можливість для більш швидкої обробки інформації і більш швидкісної передачі даних між системами. У 80-х роках XX століття оператори телефонного зв'язку виявили, що неголосовий трафік більш важливий і починає домінувати над голосовим. Був запропонований дизайн ISDN, який описував цифрову мережу з комутацією пакетів, яка надає послуги телефонного зв'язку і передачі даних. Оптоволокно дозволяло забезпечити передачу даних на високій швидкості з малими втратами. Але технологія комутації пакетів не забезпечувала надійну передачу голосу, і багато хто

сумнівався, що коли-небудь забезпечить. На противагу мережам пакетної передачі даних в громадських телефонних мережах застосовували технологію комутації каналів. Ця технологія ідеальна для передачі голосу, але для передачі даних вона неефективна. І тоді телекомунікаційна індустрія звернулася до ITU для розробки нового стандарту для передачі даних і голосового трафіку в мережах з широкою смугою пропускання. В кінці 80-х Міжнародним телефонним і телеграфним консультативним комітетом CCITT (який потім був перейменований в ITU-T) був розроблений набір рекомендацій по ISDN другого покоління, так званого B-ISDN (широкосмуговий ISDN), розширення ISDN. Як режим передачі нижнього рівня для B-ISDN був обраний ATM. У 1988 р. на зборах ITU в Женеві була обрана довжина комірки ATM — 53 байт. Це був компроміс між американцями, які хотіли розмір даних у клітинці 64 байта і європейцями, які схилялися до розміру даних 32 байта. Жодна сторона не змогла виграти в цій суперечці і в результаті було обрано середній розмір 48 байт. Для поля заголовка був обраний розмір 5 байт, мінімальний розмір, на який погодилася ITU. У 1990 р. був схвалений базовий набір рекомендацій ATM. Базові принципи ATM покладені рекомендацією I150. Це рішення було дуже схоже на системи розроблені Coudreuse і Fraser. Звідси починається подальший розвиток ATM.

Мережа будується на основі ATM комутатори та ATM маршрутизатора. Технологія реалізується як в локальних, так і в глобальних мережах. Допускається спільна передача різних видів інформації, включаючи відео, голос.

Осередки даних, що використовуються в ATM, менше в порівнянні з елементами даних, які використовуються в інших технологіях. Невеликий, постійний розмір комірки, використовуваний в ATM, дозволяє:

– передавати дані по одним і тим же фізичним каналах, причому як при низьких, так і при високих швидкостях;

– працювати з постійними і змінними потоками даних;

– інтегрувати будь-які види інформації: тексти, мова, зображення, відеофільми;

– підтримувати з'єднання типу точка-точка, точка-безліч, безліч-безліч.

Технологія ATM передбачає міжмережна взаємодія на трьох рівнях.

Для передачі даних від відправника до одержувача в мережі ATM створюються віртуальні канали, VC (англ. Virtual Circuit), які бувають трьох видів:

– постійний віртуальний канал, PVC (Permanent Virtual Circuit), що створюється між двома точками і існує протягом тривалого часу, навіть за відсутності даних для передачі;

– комутований віртуальний канал, SVC (Switched Virtual Circuit), що створюється між двома точками безпосередньо перед передачею даних і розривається після закінчення сеансу зв'язку;

– автоматично настроюється постійний віртуальний канал, SPVC (Soft Permanent Virtual Circuit).

Канали SPVC по суті представляють собою канали PVC, які не започатковано на вимогу в комутаторах ATM. З точки зору кожного учасника з'єднання, SPVC виглядає як звичайний PVC, а що стосується комутаторів ATM в інфраструктурі провайдера, то для них канали SPVC мають значні відмінності від PVC. Канал PVC створюється шляхом статичного визначення конфігурації в рамках всієї інфраструктури провайдера і завжди знаходиться в стані готовності. Але в каналі SPVC з'єднання є статичним тільки від кінцевої точки (пристрій DTE) до першого комутатора ATM (пристрій DCE). А на ділянці від пристрою DCE відправника до пристрою DCE одержувача в межах інфраструктури провайдера з'єднання може формуватися, розриватися і знову встановлюватися на вимогу. Встановлене з'єднання продовжує залишатися статичним до тих пір, поки порушення роботи однієї з ланок каналу не викличе припинення функціонування цього віртуального каналу в межах інфраструктури провайдера мережі.

Для маршрутизації в пакетах використовують так звані ідентифікатори пакета. Вони бувають двох видів:

– VPI (англ. virtual path identifier) - ідентифікатор віртуального шляху (номер каналу);

– VCI (англ. virtual circuit identifier) - ідентифікатор віртуального каналу (номер з'єднання).

Визначено п'ять класів трафіку, що відрізняються наступними якісними характеристиками:

– наявністю або відсутністю пульсації трафіку, тобто трафіки CBR або VBR;

– вимогою до синхронізації даних проміжній сторонами;

– типом протоколу, що передає свої дані через мережу ATM, — з встановленням з'єднання або без встановлення з'єднання (тільки для випадку передачі комп'ютерних даних).

CBR не передбачає контролю помилок, управління трафіком або який-небудь іншої обробки. Клас CBR придатний для роботи з мультимедіа реального часу.

Клас VBR містить у собі два підкласи — звичайний і для реального часу (див. таблицю нижче). ATM в процесі доставки не вносить ніякого розкиду осередків по часу. Випадки втрати осередків ігноруються. Клас ABR призначений для роботи в умовах миттєвих варіацій трафіку. Система гарантує деяку пропускну здатність, але протягом короткого часу може витримати і велике навантаження. Цей клас передбачає наявність зворотного зв'язку між приймачем і відправником, яка дозволяє знизити завантаження каналу, якщо це необхідно.

Клас UBR добре придатний для посилки IP-пакетів (немає гарантії доставки і в разі перевантаження неминучі втрати).

1.3 Протоколи маршрутизації

В даній роботі розглянуто векторно-дистанційний протокол RIP, EIGRP протоколи стану каналу передачі OSPF та IS-IS, а також розглянуто протокол зовнішнього шлюза BGP.

1.3.1 Routing Information Protocol version 2

RIP є векторно-дистанційним протоколом маршрутизації, в якій за метрику використовується кількість переходів. Інтервал утримання становить 180 секунд. RIP перешкоджає утворенню петель маршрутизації шляхом впровадження обмежень на кількість переходів на шляху від джерела до пункту призначення. Стандартна максимальна кількість переходів становить 15 хопів. Цей показник також обмежує розмір мережі, підтримуваний цим протоколом. Кількість хопів 16 вважається нескінченною відстанню і використовується для видалення маршруту із процесу відбору найкращого шляху.

Приклад мережі RIP зображено на рисунку 1.1.

RIP має механізми «роздвоєння горизонту», «отруєння маршруту» для запобігання розповсюдження неправильної інформації маршрутизації. Ось деякі з особливостей стабільності RIP. Крім того, можна використовувати алгоритм визначення топології на основі метрик RMTI . За його допомогою можна виявити всі можливі петлі з невеликими витратами процесорного часу.

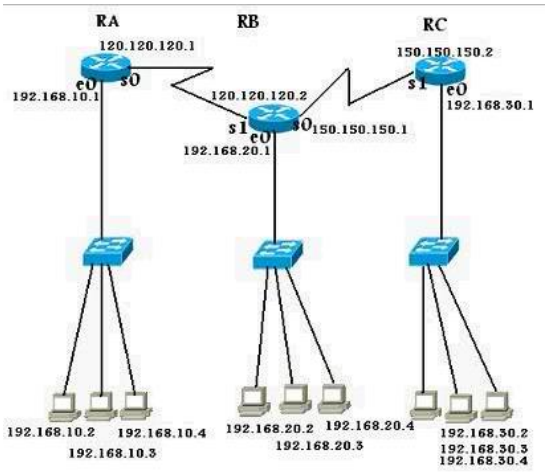

Рисунок 1.1 – Приклад мережі RIP

Спочатку кожен RIP-маршрутизатор передавав повне оновлення кожні 30 секунд. На початку впровадження протоколу, таблиці маршрутизації були досить маленькими, отже згенерований трафік не був значним. Оскільки мережі зростали в розмірах, стало очевидно, що даний підхід є дуже неефективним, навіть якщо маршрутизатори були ініціалізовані у випадкові моменти часу. Вважалося, що в результаті випадкової ініціалізації поновлення маршрутів буде поширено в часі, але це не так на практиці. Sally Floyd і Van Jacobson показали в 1994 р. , що за невеликої рандомізації таймерів оновлення, вони синхронізувалися з плином часу.

У більшості поточних мережевих середовищах, RIP не є кращим вибором для маршрутизації, бо він потребує відносно багато часу для конвергенції мережі і є менш масштабованим у порівнянні з EIGRP, OSPF або IS-IS, а також (без RMTI) обмеженість кількості переходів серйозно обмежує розмір мережі, що може підтримуватися. Однак, RIP є найпростішим у використанні, так як не потребує ніяких параметрів на маршрутизаторі на відміну від інших протоколів.

На рисунку 1.2 зображено формат RIP Entry.

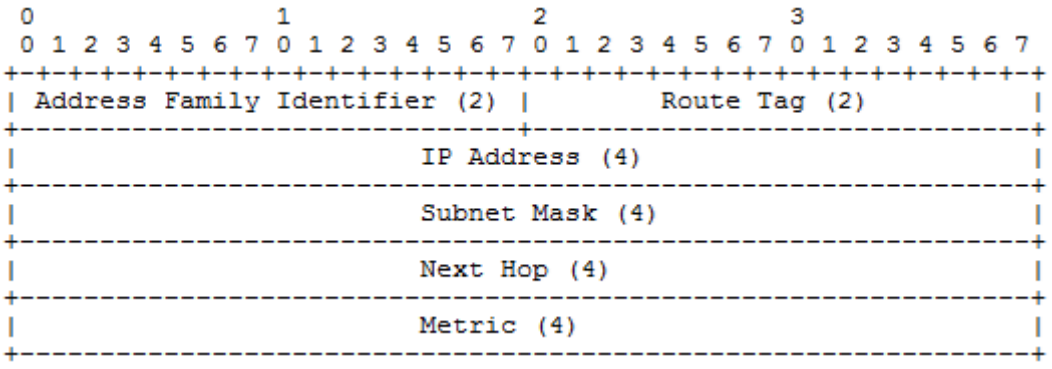

Рисунок 1.2 – Формат RIP Entry для протоколу RIP-2

Розшифрування елементів RIP Entry:

– Address Family Identifier — (AFI) Тип адреси, звичайно підтримується тільки запис AF_INET, яке дорівнює 2 (тобто використовується для протоколу IP);

– Route Tag — (RT) Тег маршруту. Призначений для поділу «внутрішніх» маршрутів від «зовнішніх», взяті наприклад з іншого IGP або EGP;

– IP Address — IP адреса місця призначення;

– Subnet Mask — Маска під мережі;

– Next Hop — Наступний хоп. Містить IP-адресу маршрутизатора на шляху до місця призначення. Значення 0.0.0.0 — хопом до місця призначення є відправник пакета;

– Metric — Метрика маршруту.

У якості транспортного протоколу RIP використовує UDP. Зарезервований номер порту - 520.

1.3.2 Extended Interior Gateway Routing Protocol

EIGRP є пропрієтарним протоколом корпорації Cisco та розроблений на базі протоколу IGRP. EIGRP є розширеним векторно-дистанційним протокол маршрутизації, оптимізований для мінімізації нестабільності маршрутизації після змін топології та ефективного використання смуги пропускання і обчислювальних потужностей маршрутизатора. Маршрутизатори, які підтримують протокол EIGRP автоматично поширюють інформацію про маршрути до IGRP-сусідів шляхом перетворення 32 біт EIGRP метрики до 24 біт IGRP метрики. На рисунку 1.3 зображено приклад мережі EIGRP.

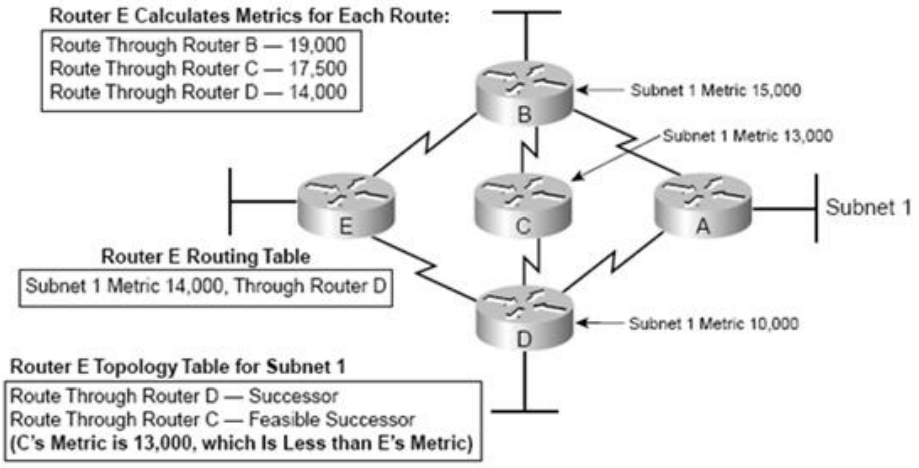

Рисунок 1.3 – Приклад мережі EIGRP

На відміну від більшості інших векторно-дистанційних протоколів, EIGRP передає повні дампи таблиці маршрутизації тільки при ініціалізації нового сусіда, а в послідуючому обмежується передачею змін в зазначеній таблиці. Це має дуже вагомий позитивний вплив на швидкість конвергенції, на навантаження мережі службовим трафіком та на використання обчислювальних потужностей маршрутизатора.

Основним алгоритмом обробки отримуваних маршрутів є Diffusing Update Algorithm (DUAL). Його завданням є обрахунок всіх отримуваних від сусідів маршрутів, та вибірка двох типів маршрутів: «спадкоємець» та «можливий спадкоємець».

Алгоритм DUAL використовує три таблиці:

– Таблиця сусідів – зберігає інформацію, отримувану від сусідів. Кожна рядок відповідає сусіду та містить назву інтерфейсу, адресу та значення таймеру утримання.

– Таблиця топології – зберігає інформацію про «спадкоємців», «можливих спадкоємців», що включає:

1. feasible distance – метрика, вирахувана локальним маршрутизатором;
2. reported distance – метрика, вирахувана на сусідньому маршрутизаторі та передана у складі update-повідомлення;
3. route status – статус маршруту, можливі два значення: а
   - активний – маршрут обробляється алгоритмом або недоступний;
   - пасивний – стабільний маршрут, який може бути використаний для передачі даних.

– Таблиця маршрутизації – зберігає найкращий маршрут по кожному префіксу. Вибираються із «спадкоємців» в таблиці топології.

EIGRP підтримує безкласову міждоменну маршрутизацію (CIDR), що дозволяє використовувати маски підмереж змінної довжини.

EIGRP підтримує окремі процеси маршрутизації для Інтернет-протоколу (IP), IPv6, IPX і AppleTalk за допомогою протоколо-залежних модулів (PDMS).

1.3.3 Протокол Open Shortest Path First

OSPF є адаптивним протоколом маршрутизації для IP-мереж. Він використовує алгоритм Дейкстри і потрапляє в групу внутрішніх протоколів маршрутизації, що працюють в рамках однієї автономної системи (AS). Визначений як OSPF версії 2 в RFC 2328 (1998) для IPv4. Оновлення для IPv6 визначено як OSPF версії 3 в RFC 5340 (2008).

OSPF, мабуть, найільш широковикористовуваний протокол внутрішньої маршрутизації (IGP) у великих корпоративних мереж. IS-IS, інший протокол стану каналу, частіше зустрічається у великих мережах постачальників послуг доступу до Інтернет.

OSPF є протоколом внутрішнього шлюзу, що маршрутизує пакети інтернет-протоколу (IP) виключно в межах одного домену маршрутизації (автономної системи). Він збирає інформацію про стан каналів з наявних маршрутизаторів і будує карту топології мережі. Топологія визначає таблицю маршрутизації рівня Інтернет по моделі OSI, що робить рішення щодо пересилки, заснованим виключно на IP-адресі призначення, що знаходиться в IP-пакеті. OSPF був розроблений з підтримкою моделі безкласової міждоменної маршрутизації (CIDR).

OSPF виявляє зміни в топології, такі як збої з'єднання, дуже швидко і обчислює нову структуру маршрутизації в мережі протягом декількох секунд. Він обчислює дерево з найкоротшим шляхом для кожного маршруту з допомогою методу, заснованого на алгоритмі Дейкстри “Shortest Path First“. Інформація про стан каналу зберігається на кожному маршрутизаторі, як база даних станів (LSDB), яка являє собою дерево-образ всієї топології мережі. Ідентичні копії LSDB періодично оновлюються через передачу об’яв стану каналу на всіх маршрутизаторах OSPF.

OSPF політики маршрутизації для побудови таблиці маршрутизації регулюються вартостями каналів (зовнішніх метрик), пов'язаних з кожним інтерфейсом маршрутизації. Такими факторами можуть бути відстань до

маршрутизатора (час прийому-передачі), пропускна здатність каналу зв’язку, або доступність з'єднань і надійність, виражена в безрозмірних числах. Це забезпечує динамічний процес балансування трафіку між маршрутами рівної вартості.

Мережі OSPF можуть бути структуровані в області маршрутизації, щоб спростити адміністрування і оптимізувати трафік і використання ресурсів. Райони ідентифікуються за допомогою 32-розрядних чисел, виражається або в десятковій системі, або в октетах розділених точками, на кшталт позначення IPv4 адрес. На рисунку 1.4 зображено приклад мережі OSPF.

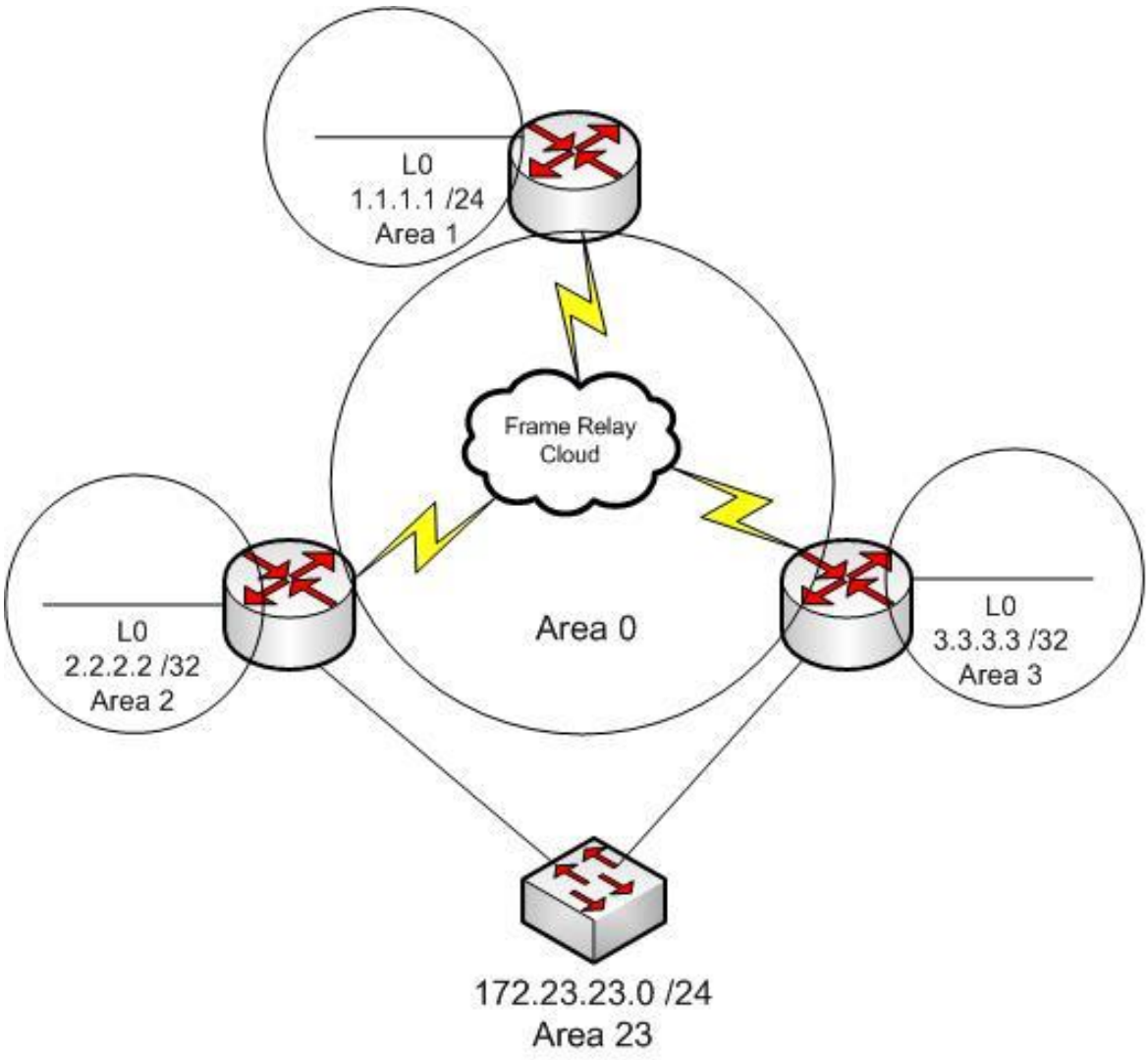

Рисунок 1.4 – Приклад мережі OSPF

Відповідно до угоди, площа 0 (нуль) або 0.0.0.0 представляє ядро або основу області OSPF мережі. Номера інших областей можуть бути обрані за бажанням, але найчастіше за ідентифікатор береться IP-адреса основного маршрутизатора в області. Кожна додаткова область повинна мати пряме чи віртуальне з'єднання з головною областю OSPF. Такі зв'язки підтримуються з'єднувальним маршрутизатором, відомим як граничний маршрутизатор області (ABR). ABR підтримує веде окремі бази даних про стан каналу для кожної області, а також зберігає узагальнені маршрути по всіх областях в мережі.
OSPF не використовує стек протоколів TCP / IP (UDP, TCP), а інкапсулює свої повідомлення безпосередньо в IP-пакети з номером протоколу 89. OSPF володіє власними механізмами виявлення та виправлення помилок.

OSPF використовує групову адресацію для розповсюдження своїх повідомлень. Для мереж, які не підтримують групову адресацію використовуються спеціальні механізми визначення сусідів. Багатоадресні пакети OSPF ніколи не перетинають IP-маршрутизатори, тому що встановлена межа переходу в 1 хоп. OSPF залишає за собою групові адреси 224.0.0.5 для IPv4 або FF02:: 5 для IPv6 (усі SPF маршрутизатори, також відомий як AllSPFRouters) і 224.0.0.6 для IPv4 або FF02:: 6 для IPv6 (для головних (designated) маршрутизаторів, AllDRouters) , як зазначено в RFC 2328 і RFC 5340.

Для маршрутизації багатоадресного трафіку IP, OSPF підтримує Multicast OSPF, як визначено в RFC 1584. Ні Cisco, ні Juniper Networks не підтримують MOSPF в своїх реалізаціях OSPF. У поєднанні з OSPF широко використовується PIM (Protocol Independent Multicast).

Протокол OSPF, при роботі з IPv4, може працювати безпечно між маршрутизаторами, при необхідності використовуючи різні методи аутентифікації, щоб тільки довірені маршрутизатори приймали участь в маршрутизації. OSPFv3, що працює на IPv6, більше не підтримує протоколу внутрішньої аутентифікації. Натомість він покладається на протокол безпеки IPsec.

1.3.4 Протокол Intermediate System To Intermediate System

Протокол IS-IS є протоколом маршрутизації, що призначений для ефективного переміщення інформації в комп'ютерній мережі, групи фізично підключених комп'ютерів або подібних пристроїв. Це досягається шляхом визначення оптимального маршруту для датаграми через мережу з комутацією пакетів. Протокол був визначений у ISO / IEC 10589:2002 в якості міжнародного стандарту в рамках взаємодії відкритих систем (OSI) еталонного дизайну. Хоча спочатку протокол був стандартизований ISO, IETF перевидав протокол як стандарт Інтернету в RFC 1142. IS-IS був названий де-факто стандартом для великих магістралей постачальника мережевих послуг. На рисунку 1.5 зображено приклад мережі IS-IS.

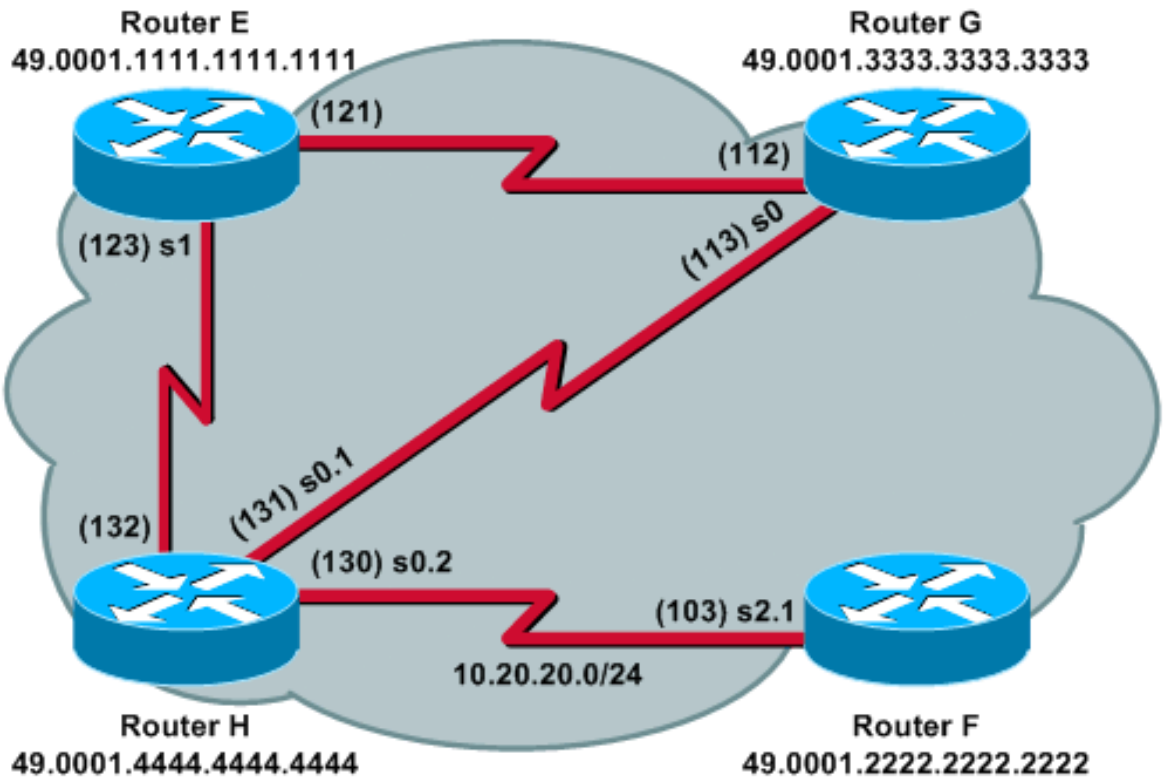

Рисунок 1.5 – Приклад мережі IS-IS

IS-IS є протоколом внутрішнього шлюзу, спроектованим для використання в межах адміністративного домену або мережі. По типу функціонування являє

собою протоколом стану каналу зв'язку. На кожному IS-IS маршрутизаторі незалежно будується таблиця мережевої топології, на основі прийнятої від інших IS-IS маршрутизаторів мережевої інформації. Цей протокол використовує алгоритм Дейкстри для побудови графу топології мережі, що надає змогу уникнути утворенню «петель» на шляху передачі пакетів.

Протокол IS-IS був розроблений американською корпорацією Digital Equipment Corporation як частина п'ятої фази впровадження мережі DECnet. Був стандартизований ISO в 1992 році, як стандарт ISO 10589 для комунікації між проміжними мережевими пристроями.

Розробка протоколу проводилась з метою отримати динамічний протокол маршрутизації датаграм протоколу CLNS (Connectionless Network Service). Протокол був розроблений приблизно в той же час, коли Internet Enginnering Task Force розробляла протокол OSPF, описаний вище. Пізніше IS-IS був розширений для підтримки IP-мереж. Ця версія протоколу отримала назву Integrated IS-IS (RFC 1195).

Концептуально IS-IS дуже схожий з протоколом OSPF, тому що вони обидва використовують алгоритм Дейкстри для побудови топологічного графа, підтримують адресування з використанням масок змінної довжини, можуть використовувати групову адресацію для виявлення сусідніх роутерів користуючись повідомленнями Hello, а також підтримують аутентифікацію повідомлень Routing Update.

На відміну від OSPF, який при розробці був орієнтований на IP-мережі, протокол IS-IS розроблявся для роботи в мережах CLNS. IS-IS не використовує IP для виконання маршрутизації інформаційних повідомлень. IS-IS є нейтральним щодо типу мережевих адрес, для яких він може маршрутизувати. OSPF, з іншого боку, був розроблений для IPv4. Це дозволило IS-IS бути легко адаптованим для роботи з IPv6. Для роботи з мережами IPv6, протокол OSPF був переписаний у OSPF v3 (RFC 2740).

IS-IS маршрутизатори будують топологічне подання мережі. Ця карта вказує які підмережі кожний IS-IS маршрутизатор може досягти, а найнижча

вартість (найкоротший) шлях до підмережі використовується для перенаправлення трафіку.

IS-IS відрізняється від OSPF у визначенні зони та маршрутизуванні між зонами. IS-IS маршрутизатори поділяються на три рівні:

– Рівень 1 – всередині виділеної зони;

– Рівень 2 – всередині «основної» («хребтової») зони;

– Рівень 1-2 – може знаходитися всередині зон обох зазначених вище типів.

Маршрутизатори другого рівня можуть формувати відносини тільки з іншими маршрутизаторами 2-го рівня. Обмін інформацією відбувається між роутерами першого рівня, або між роутерами другого рівня. Рівень 1-2 маршрутизатори обмінюються інформацією з обох рівнях і використовуються для взаємодії маршрутизаторів другого рівня з маршрутизаторами всередині області.

У OSPF граничний маршрутизатор області (ABR) насправді знаходиться в двох або кількох областях одночасно, ефективно створюючи кордон між областями всередині ABR, тоді як в IS-IS район кордону між маршрутизаторами 2-го рівня або рівня 1-2. В результаті, IS-IS маршрутизатор є може бути частиною тільки однієї області. IS-IS також не потребує зони 0 для магістральної області, через яку весь міжзональний трафік повинен пройти. Коли OSPF створює мережу на кшталт зіркової топології, де багато областей підключені безпосередньо до області нуля, IS-IS, створює логічну топологію, де другий рівень є основним, до якого під'єднуються маршрутизатори першого або 1-2 рівня, формуючи окремі області.

OSPF має більший набір розширень і додаткових функцій. Однак IS-IS може масштабуватися для підтримки більш великих мереж. Використовуючи однаковий набір ресурсів, IS-IS може підтримувати більшу кількість маршрутизаторів в області, ніж OSPF. Це сприяло тому становленню IS-IS, як протоколу масштабу провайдера мережевих послуг.

TCP / IP реалізація, відома як "Integrated IS-IS" або "Dual IS-IS", описана у документі RFC 1195.

1.3.5 Border Gateway Protocol

Протокол граничного шлюзу (BGP) є протоколом, приймаючим основні рішення щодо маршрутизації в мережі Інтернет. Він підтримує таблицю IP-мереж або "префіксів", які визначають доступність мереж між автономними системами. Він вважається протоколом вектора шляху. BGP не використовує традиційні Interior Gateway Protocol (IGP), метрики, але робить рішення про маршрутизації на основі шляху, мережевих політик та/або наборів правил. З цієї причини, його можна було б називати протоколом досяжності, а не протоколом маршрутизації.

BGP був створений для заміни Exterior Gateway Protocol (EGP) протокол, для підтримки децентралізованої маршрутизації. А саме переходу від базової моделі ARPAnet до децентралізованою системи управління, що включає за NSFNET і пов'язані регіональні мережі. Це дозволило Інтернету стати по-справжньому децентралізованою системою. Починаючи з 1994 року, четверта версія BGP використовується в Інтернеті. В даний час всі попередні версії вважаються застарілими. Значним вдосконаленням четвертої версії була підтримка безкласової міждоменної маршрутизації і використання агрегування маршрутів, щоб зменшити розмір таблиць маршрутизації. З січня 2006 року, версія 4 закріплена у документі RFC 4271, яка пройшла через більш ніж 20 чорнових варіантів та основана на RFC 1771 версії 4. RFC 4271 виправила ряд помилок, уточнила неясності і зробила RFC набагато ближче до галузевої практики.

Більшість постачальників послуг Інтернету повинні використовувати BGP для встановлення маршрутизації між собою (особливо якщо вони мають декілька виходів до NAP). Таким чином, хоча більшість користувачів Інтернету не використовують його безпосередньо, BGP є одним з найбільш важливих

протоколів Інтернету. Порівняйте це з основною системою сигналізації 7 (SS7), який основним протоколом встановлення телефонних дзвінків у комутованій телефонній мережі загального користування. Дуже великі приватні IP-мережі також використовують BGP. Прикладом може бути приєднання ряду великих OSPF (Open Shortest Path First) мереж, де можливостей OSPF по масштабуванню не вистачає для підтримки мережі. Іншою причиною використання BGP є множинна адресація мережі для кращої надмірності або кілька точок доступу до одного (RFC 1998) або до декількох провайдерів.

BGP сусіди, встановлюються ручним налаштуванням між маршрутизаторами для створення сесії TCP на порту 179. Спікер BGP буде періодично відправляти 19-байтні Keep-Alive повідомлення для підтримки зв'язку (за замовчуванням кожні 60 секунд). Серед протоколів маршрутизації BGP єдиний використовує TCP, в якості транспортного протоколу.

BGP всередині автономної системи (AS) носить назву Internal BGP (IBGP). При роботі між автономними системами він називається зовнішнім BGP (EBGP).

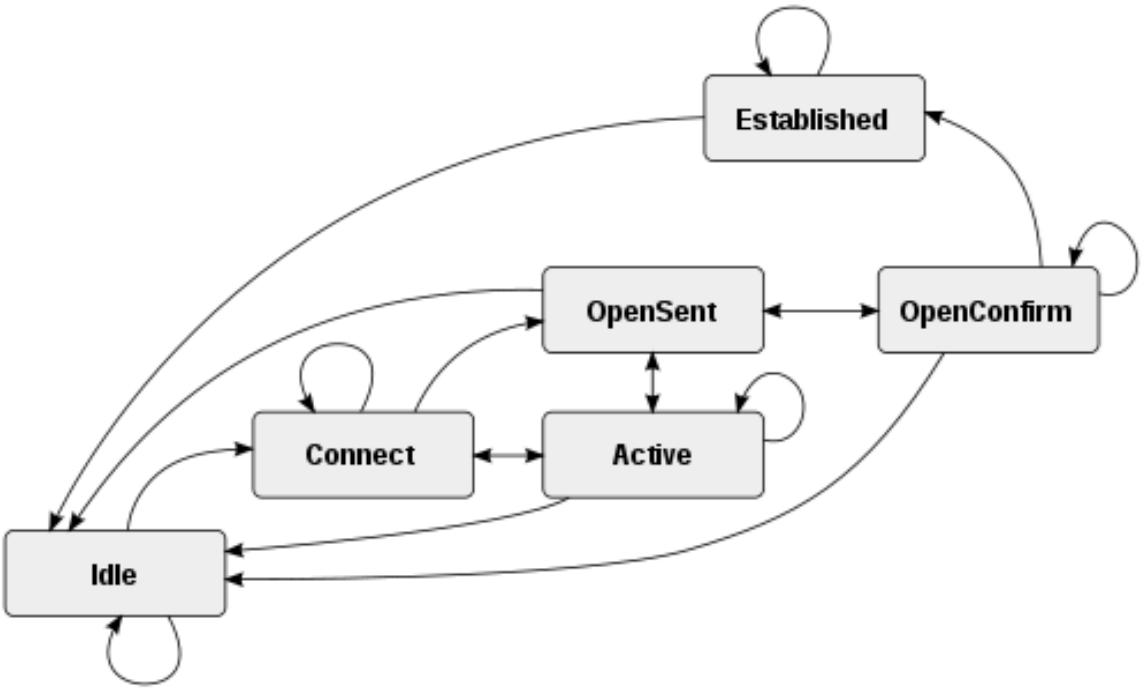

Рисунок 1.6 – Кінцевий автомат станів протоколу BGP

Маршрутизатори на кордоні однією автономної системи, що ведуть обмін інформацією з іншими автономними станціями називаються граничними маршрутизаторами. В операційній системі Cisco IOS, IBGP маршрути мають адміністративну відстань 200, який є менш привабливим, ніж маршрут, отриманий через EBGP або будь-який протокол внутрішнього шлюзу. Інші реалізації маршрутизаторів також віддають перевагу EBGP, у порівнянні з IGP або IBGP.

Для прийняття рішення в протоколі BGP використовується кінцевий автомат (FSM), зображений на рисунку 1.6, і складається з шести станів. Для кожної сесії, реалізація BGP встановляю активний стан. Також BGP визначає тип і формат повідомлень, що використовуються для зміни стану. На рисунку 1.7 зображено приклад мережі BGP.

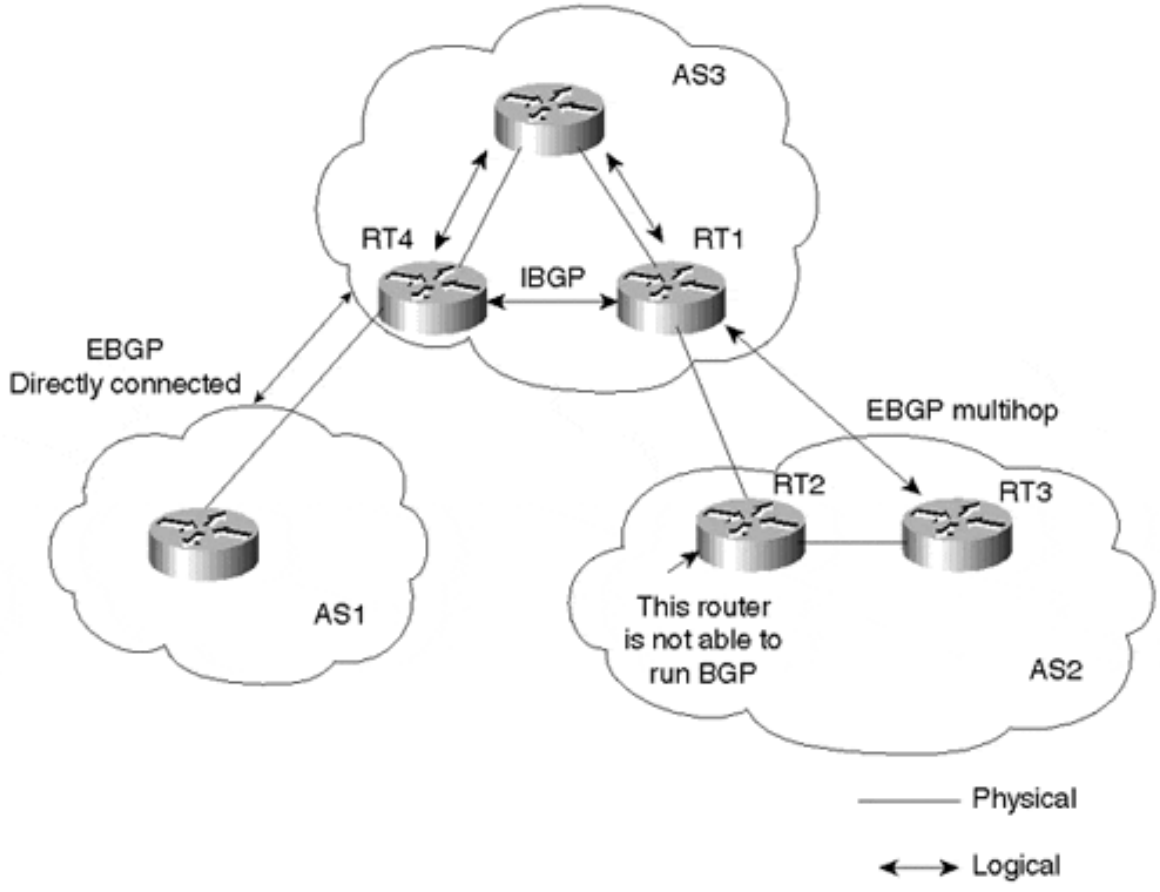

Рисунок 1.7 – Приклад мережі BGP

Основні стани кінцевого автомату, що використовується в протоколі BGP:

- Idle - BGP виділяє ресурси, відхиляє вхідні з’єднання та ініціює TCP з’єднання до піра.
- Connect – маршрутизатор чекає на успішне встановлення TCP з’єднання та перходить наступного стану.
- OpenSen” – роутер відправляє open messages та чекає на підтвердження отримання.
- Established – роутер готовий надсилати та приймати повідомлення keep-alive, update, notification.

1.4 Технологія MPLS

MPLS (англ. Multiprotocol Label Switching — багатопротокольна комутація по мітках) — механізм передачі даних, який емулює різні властивості мереж з комутацією каналів поверх мереж з комутацією пакетів.

MPLS працює на рівні, який можна було б розташувати між другим (канальним) і третім (мережевим) рівнями моделі OSI, і тому його зазвичай називають протоколом другого з половиною рівня (2.5-рівень). Він був розроблений з метою забезпечення універсальної служби передачі даних як для клієнтів мереж з комутацією каналів, так і мереж з комутацією пакетів. За допомогою MPLS можна передавати трафік самої різної природи, такий як IP-пакети, ATM, Frame Relay, SONET і кадри Ethernet. На рисунку 1.8 зображено схему розповсюдження міток по мережі MPLS.

В традиційній IP мережі пакети передаються від одного маршрутизатора до іншого й кожен маршрутизатор зчитуючи заголовок пакета (адреса призначення) приймає рішення про те, за яким маршрутом відправити пакет далі.

У протоколі MPLS ніякого подальшого аналізу заголовків в маршрутизаторах по шляху проходження не проводиться, а переадресація керується виключно на основі міток. Це має багато переваг над традиційною маршрутизацією на мережевому рівні.

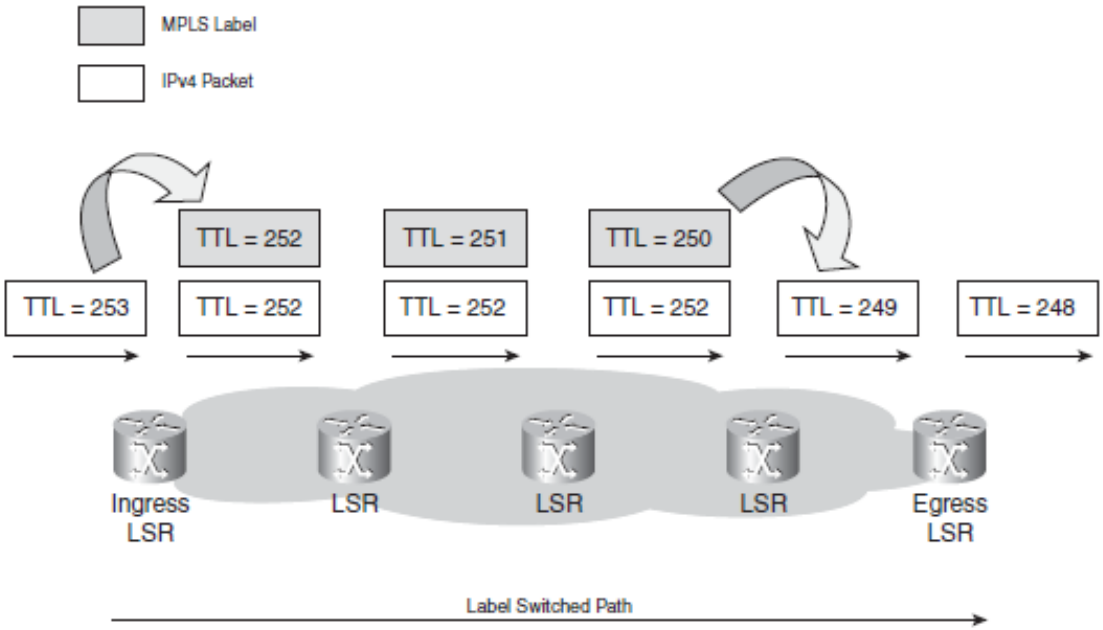

Рисунок 1.8 – Розповсюдження міток по MPLS мережі

MPLS був запропонований групою інженерів з Ipsilon Networks, але їх "IP Switching" технологія, яка була визначена тільки до роботи з мережами ATM, тому значного поширення технологія не набула. В свою чергу Cisco Systems, Inc, представив пропозицію, яка розширювала список підтримуваних типів мережі, та отримала назву "Tag Switching". Це був пропрієтарний протокол, який пізніше перейменували в "Label Switching". Вона була передана в IETF для відкритої стандартизації. IETF включали пропозиції від інших виробників, і розробляли протокол, який би об'єднай всі доступні функції в різних постачальників.

Однією з перших цілей було дозволення створення простих високошвидкісних комутаторів, так як на протязі значного періоду часу неможливо було передавати IP-пакети повністю на апаратному рівні. Тим не менш, функціонал VLSI був доступний на дуже обмеженій кількості мережевого обладнання. Тому переваги MPLS в основному обертаються навколо можливості підтримки декількох моделей надання сервісу та контроль управління маршрутами руху трафіку. MPLS також пропонує надійну технологію

відмовостійкості, яка є більш ефективної ніж технологія захисту простих кілець синхронної оптичної мережі (SONET / SDH).

1.5 Мережеве обладнання

1.5.1 Обладнання Cisco Inc.

Cisco Systems - найбільший в світі виробник мережного устаткування, призначеного для обслуговування мереж віддаленого доступу, сервісів безпеки, мереж зберігання даних,3 маршрутизації і комутації, а також для потреб комерційного ринку IP-комунікацій і корпоративного ринку.

Заснована в 1984 р. Станом на 2017 рік в компанії працюють 73 тис. чоловік по всьому світу [4].

На цей час Cisco виробляє велику кількість різноманітних пристроїв, наприклад:

- Ethernet комутатори;
- Маршрутизатори;
- Продукти для IP-телефонії, такі як IP PBX, VoIP-шлюзи;
- Пристрої мережної безпеки (міжмережні екрани, VPN, IDS тощо);
- Wi-Fi точки доступу;
- Платформи оптичної комутації;
- ATM-комутатори;
- Кабельні модеми;
- DSL-устаткування;
- Універсальні шлюзи і шлюзи віддаленого доступу;
- Комутатори мереж зберігання даних (SAN, Storage Area Network);
- Програмне забезпечення управління мережею.

Cisco називає себе «світовим лідером в області мережних технологій, призначених для мережі Інтернет».

У 2003 Cisco придбала фірму Linksys, популярного виробника устаткування для комп'ютерних мереж і тепер позиціонує торгову марку Linksys як мережне устаткування для домашнього використання і малого бізнесу.

Використовуючи придбання компаній, внутрішні розробки і партнерство з іншими компаніями, Cisco вийшла на ринок IP-телефонії з своїми IP-телефонами, менеджерами викликів і шлюзами до телефонної мережі загального користування. Раніше Cisco вийшла на ринок ATM-обладнання з придбанням в 1996 році фірми StrataCom Inc.

В грудні 2009 р. Cisco стала власником більш ніж 90% акцій норвезької компанії Tandberg, що дозволить Cisco стати світовим лідером в виробництві обладнання для відеоконференцій.

Подружня пара Леонард Босак (Leonard Bosack) і Сандра Лернер (Sandra Lerner) заснувала компанію Cisco Systems в 1984 році. Вони працювали як обслуговуючий комп'ютерний персонал в Стенфордському університеті. Леонард Босак адаптував безліч програм маршрутизатора протоколів, написаних Вільямом Іджером (William Yeager), іншим працівником, який почав роботу за декілька років до приходу Босака з Пенсільванського Університету, де він отримав ступінь бакалавра.

Хоча Cisco не була першою компанією, що розробляла і продавала маршрутизатори, — пристрої, що перенаправляють комп'ютерний трафік з однієї мережі в іншу, — вона створила перший комерційно успішний багатопротокольний маршрутизатор. Це пристрій, що дозволяв раніше несумісним комп'ютерам спілкуватися між собою, навіть якщо вони використовували різні мережні протоколи.

У 1990 Босак і Лернер пішли з компанії з 170 мільйонами доларів після того, як венчурні інвестори ввели до складу правління професійних менеджерів. Пізніше Босак і Лернер розвелися.

Назва Cisco — скорочення від назви міста Сан-Франциско, штат Каліфорнія (San Francisco). Раніше, коли засновники вибирали для компанії назву, вони часто потрапляли на імена, які вже зайняті або використовуються.

Врешті-решт хтось запропонував назву «cisco» з першою маленькою буквою «c» (вже існувала компанія з назвою «CISCO»). Існує версія, згідно з якою первинна назва компанії звучала і писалася саме як San-Francisco Systems, але в процесі реєстрації ніяковий рух адвоката (або нотаріуса) привів до надриву титульного листа з назвою компанії. Майбутні власники визнали це за знак і зафіксували назву cisco Systems з маленької букви.

Ім'я ciscoSystems (з маленькою «c») продовжувало використовуватися в співтоваристві інженерів компанії ще довго після того, як компанія офіційно змінила ім'я на Cisco Systems, Inc. Назву «ciscoSystems» досі можна зустріти в повідомленнях IOS і звітах про помилки.

Обладнання Cisco відповідає всім вимогам безпеки, і тому його закладено в основу національної системи конфіденційного зв’язку, яка об’єднує всі міністерства та відомства України в єдину захищену мережу. Технології Cisco широко застосовуються у різних державних установах та муніципальних службах, у закладах освіти та охорони здоров’я.

Провідні українські корпорації – фінансові установи, виробничі підприємства та енергетичні компанії – ґрунтують свою IT-стратегію на базі архітектурних концепцій Cisco.

Малі та середні підприємства за допомогою технологій Cisco підвищують свою конкурентоспроможність та забезпечують свій розвиток. А українські оператори зв’язку: «Укртелеком», Utel, «Київстар», «МТС», «Голден-Телеком», «Датагруп» та багато інших – використовують рішення Cisco для розбудови власної інфраструктури нового покоління, щоб забезпечити для користувачів всієї країни якісні телекомунікаційні послуги.

Компанія Cisco є одним з лідерів та законодавців у сфері світової стандартизації: все устаткування Cisco успішно проходить необхідні тестування, про що свідчить наявність міжнародних сертифікатів ISO та Declaration of Conformity. Так само компанія приділяє велику увагу проведенню в різних країнах окремої сертифікації на відповідність місцевим вимогам і технологічним особливостям.

В Україні все обладнання Cisco успішно проходить сертифікацію на відповідність системі УКРСЕПРО та її основним вимогам у сфері електромагнітної сумісності, безпеки та телекомунікаційних інтерфейсів. Устаткування Cisco також проходить сертифікацію у сфері технічного захисту інформації. Отримані від ДССЗЗІ (Державна служба спеціального зв'язку і захисту інформації) експертні висновки щодо устаткування Cisco підтверджують його відповідність основним критеріям захисту інформації.

1.5.2 Обладнання Juniper Networks

Juniper Networks - виробник обладнання для операторських мереж IP / MPLS; один з небагатьох на ринку інтелектуальних операторських рішень, що самостійно розробляє основні апаратні компоненти своїх пристроїв. На обладнанні Компанії успішно реалізуються основні інтелектуальні елементи сучасної операторської мережі (широкосмугова агрегація, міські мережі, мультисервісна межа, магістраль) із максимальною якістю. Як результат - багаторазове зростання продажів за останні декілька років, особливо на ринках країн СНД.

Пропрацювавши 11 років у дослідницькому центрі компанії Xerox PARC, Прадіп Сінді вирішив взяти відпустку, щоб подумати про своє майбутнє. Прогнозуючи швидкий розвиток мережі Інтернет і виняткову важливість можливості з'єднання комп'ютерів між собою, Сінді був вражений величезним потенціалом ринку маршрутизаторів, які є основними будівельними блоками мереж.

Після декількох невдалих спроб переговорів з венчурними фондами Сінді все ж зміг забезпечити фінансування своєї нової компанії, і Juniper Networks була зареєстрована в Каліфорнії 6 лютого 1996.

На відміну від багатьох інших стартапів, що віддають перевагу починати з малого, співробітники компанії Juniper відразу взялися за вирішення складної

проблеми. Незабаром завдання було вирішено, і такий підхід до ведення бізнесу став фірмовим стилем компанії.

В результаті у вересні 1998 року був випущений перший продукт компанії - революційний маршрутизатор M40. Маршрутизатор M40 за своїми характеристиками значно перевершував всі представлені на ринку пристрої цього класу, і компанія Juniper відразу зарекомендувала себе як серйозного і відкритого для інновацій гравця на ринку комп'ютерного обладнання.

Розробка M40 була серйозним завданням, яка вимагала двох років напружених досліджень і праці. У цей період часу для задоволення потреб венчурних фондів і замовників, в компанії Juniper була розроблена операційна система JUNOS, що згодом стала фундаментом для майбутніх інновацій і головною відмінністю компанії від інших підприємств галузі.

Після успішного старту компанія Juniper продовжує рости і залишатися лідером в області високопродуктивних мереж завдяки випуску нових продуктів і нових технологій, покликаним вирішити проблеми клієнтів.

Juniper Networks є лідером ринку за частиною інновацій, тому Juniper може забезпечити безпечну мережеву інфраструктуру, від якої залежить реалізація стратегії організації. Успіхи Juniper багаторазово підтверджені: інтегровані мережі, рішення з інформаційної безпеки та прискоренню роботи додатків вирішують найскладніші проблеми в індустрії. Більше 20 000 клієнтів, включаючи найбільших операторів зв'язку, довіряють інновацій компанії Juniper, використовуючи її інтегровані мережеві рішення для надання кращих послуг для своїх користувачів з мінімальними витратами.

1.6 Аналіз вимог

Завданням даної роботи є побудова корпоративної мережі на основі технології комутації за мітками Multiprotocol Label Switching (MPLS).

Ядро розроблюваної мережі складатися з декількох Label Routing Swich, та декількох Edge Router. Дана вимога пов'язана з необхідністю забезпечити механізмі відмовостійкості ядра мережі. В разі виходу зі строю одного або декількох маршрутизаторів, мережа повинна залишатися операбельною. В результаті робота користувачів мережі не повинна бути уражена при наявності тимчасових збоїв на окремих частинах мережі.

Також архітектура мережі повинна бути спроектована таким чином, щоб кожний критичний елемент в мережі мав заступника, який може прийняти на себе всі необхідні функції в автоматичному режимі.

Спроектована мережа повинна забезпечити високоефективний та безпечний транспорт даних користувачів мережі, які знаходяться в різних департаментах підприємства.

Безпека та конфіденціальність транспортованих даних забезпечується за допомогою декількох методик та технологій. Перш за все доступ до адміністративних ліній всіх маршрутизаторів повинен бути доступним тільки авторизованим особам. По друге, трафік між департаментами повинен підпорядковуватися правилам маршрутизації.

Ще однією, не менш важливою, вимогою є висока масштабованість мережі. Наразі об'єм трафіку на підприємстві має тенденцію до зростання, отже з часом може з'явитися необхідність в розширенні мережі.

Інформація маршрутизації, доступна на маршрутизаторах Customer Edge повинна бути імпортована до ядра мережі.

Також треба забезпечити можливість обміну трафіком з мережею Інтернет. Для цього потрібно обмінюватися інформацією маршрутизатора з обладнанням провайдера, або напряму з точкою доступу до мережі NAP (Network Access Point). Також треба розглянути можливість та доцільність підключення до двох різних провайдерів мережевих послуг для диверсифікації зв'язку до мережі Інтернет.

2 РОЗРОБКА АРХІТЕКТУРИ ТА ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

Розробка моделі мережі була розпочата з планування ядра мережі MPLS, що складається з Provider Routers, або Label Switching Routers. Було вирішено скласти ядро мережі з п’яти маршрутизаторів.

В якості протокола обміну мітками було розглянуто два протоколи:

– Tag Switching Protocol;

– Label Swithing Protocol.

Протокол розподілу міток (LDP) являє собою протокол, в якому два маршрутизатори Label Edge (LEP) обмінюються мітками інформації. Два маршрутизатори, які здійснюють обмін інформацією є двонаправленими пірами. LDP використовується для створення і підтримки LSP баз даних, які використовуються для передачі трафіку через мережу комутації по мітках (MPLS).

LDP може бути використаний для розповсюдження внутрішньої (VC / VPN / мітка послуги) та зовнішньої мітки (шлях мітки) в MPLS. Для внутрішньої розсилки міток, цільове LDP (tLDP) не використовується. LDP і tLDP виявлення працюють на UDP порту 646,а сесії встановлюються на TCP-порту 646. У стадії відкриття Hello пакети надсилаються на UDP порт 646 для "всіх маршрутизаторів в цій підмережі" до групи р груповою адресою (224.0.0.2). Тим не менш, tLDP unicast hello пакети можуть бути використані для встановлення сесії з конкретним сусідом. На рисунку 2.1 зображено схему встановлення сесії LDP.

В результаті було обрано більш новий та функціональний протокол LDP. Далі потрібно обрати протокол маршрутизації між Provide Edge маршрутизаторами. Для цього найбільш прийнятним є залучення протоколу Border Gateway Protocol з використанням розширення Multiprocol BGP Extension.

Функція багатопротокольної BGP додає можливості BGP для багатоадресної маршрутизації політики в усьому Інтернеті і для підключення групових топологій всередині та між BGP автономних систем. Тобто,

багатопротокольної BGP є розширення BGP, який додає підтримку багатоадресної IP-маршрутизації. BGP несе два набори маршрутів, один набір для індивідуальної маршрутизації і один набір для багатоадресної маршрутизації. Маршрути, пов'язані з багатоадресною маршрутизацією використовуються протоколом Independent Multicast (PIM) для побудови дерев розподілу даних.

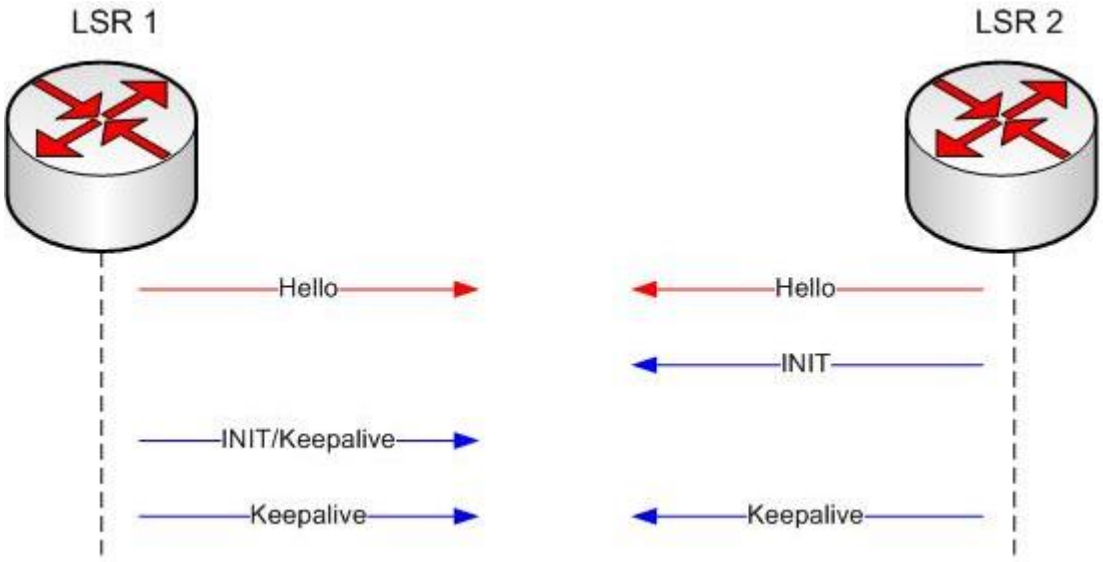

Рисунок 2.1 – Встановлення сесії LDP

Функція багатопротокольної BGP додає можливості BGP для багатоадресної маршрутизації політики в усьому Інтернеті і для підключення групових топологій всередині та між BGP автономних систем. Тобто, багатопротокольної BGP є розширення BGP, який додає підтримку багатоадресної IP-маршрутизації. BGP несе два набори маршрутів, один набір для індивідуальної маршрутизації і один набір для багатоадресної маршрутизації. Маршрути, пов'язані з багатоадресною маршрутизацією використовуються протоколом Independent Multicast (PIM) для побудови дерев розподілу даних. На рисунку 2.2 зображено приклад архітектури мережі BGP.

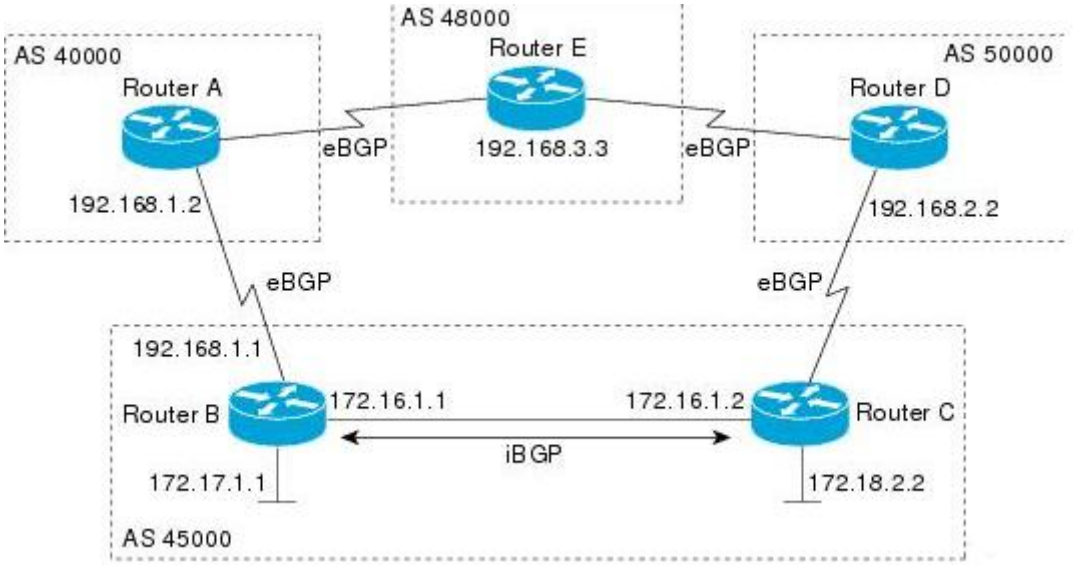

Рисунок 2.2 – Архітектура мережі BGP

Multiprotocol BGP корисний при використанні багатоадресного трафіку, а також підтримує обмеження використання ресурсів. При необхідності, щоб весь багатоадресний трафік проходив через одну точки доступу (NAP), теж використовується Multiprotocol BGP. Multiprotocol BGP дозволяє мати індивідуальну топологію маршрутизації для унікасту, та індивідуальну для групової маршрутизації. Таким чином, є більше контролю над мережею і ресурсами.

В результаті аналізу існуючих протоколів, було вирішено обрати протокол Border Gateway Protocol with Multiprotocol Extensions для обміну інформацією маршрутизації між кінцевими роутерами мережі MPLS.

При проектуванні архітектури BGP мережі було розглянуто методики забезпечення підвищеної відмовостійкості та надлишковості. Однією з таких методик є використання методики «Route Reflector» при обміні інформацією маршрутизації між BGP пірами.

Суть даного методу полягає у введені так званого «відбивача маршрутів». Маршрутизатори BGP замість підтримки з'єднань між собою, під'єднуваться до відбивача маршрутів. Таким чином, всі дані маршрутизації проходять не напряму між BGP пірами, а через концентраційну точку у вигляді відбивача

маршрутів. Даний підхід дозволить значно зменшити як загальну кількість сесій BGP, так і їх кількість на кожному окрему BGP маршрутизаторі.

Дана методика має важливу особливість. При прийнятті оновлень відбивач маршрутів запускає «процес прийняття рішення», тобто із отриманих маршрутів обирає найкращі. Таким чином загальна кількість службового трафіку, що передається в мережі, зменшиться. Також це має позитивний вплив в розрізі використання обчислювальних ресурсів BGP маршрутизаторів. На рисунку 2.3 зображено приклад архітектури мережі MBGP.

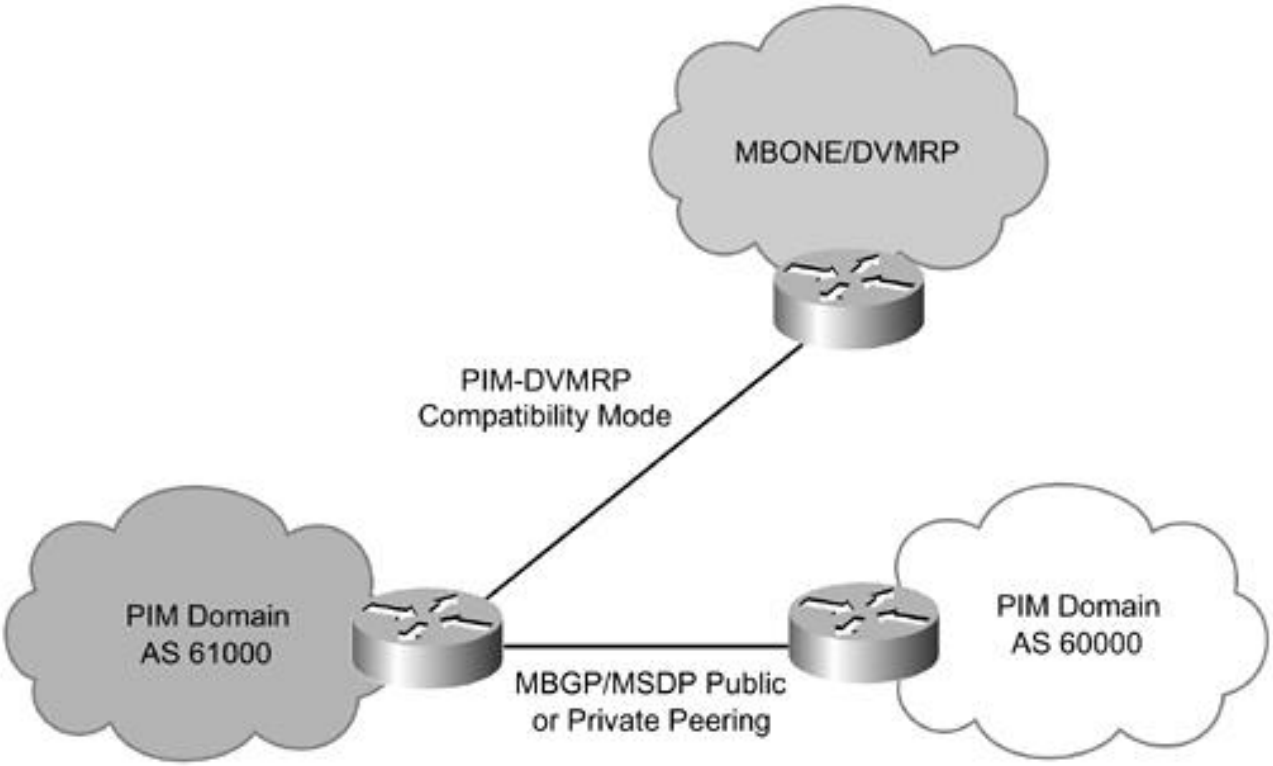

Рисунок 2.3 – Архітектура мережі з використанням MBGP

Ще однією методикою підвищення ефективності передачі інформації маршрутизації по протоколу BGP є «Confederations».

Даний метод полягає у створенні автономних систем всередині автономної системи. Тобто одна автономна система розподіляється на декілька суб-АС, які обмінюються інформацією маршрутизації між собою по протоколу EBGP. А

всередині суб-АС використовується IBGP. Для суб-АС використовуються приватні номери автономних систем.

Цей підхід має декілька мінусів. По-перше це можливість обрання неоптимального шляху транспортування трафіку, по-друге це складність конфігурування та необхідність вносити значні зміни в топологію мережі при впровадженні даного підходу. На рисунку 2.4 зображено архітектуру мережі BGP з використанням відбивачів маршрутів.

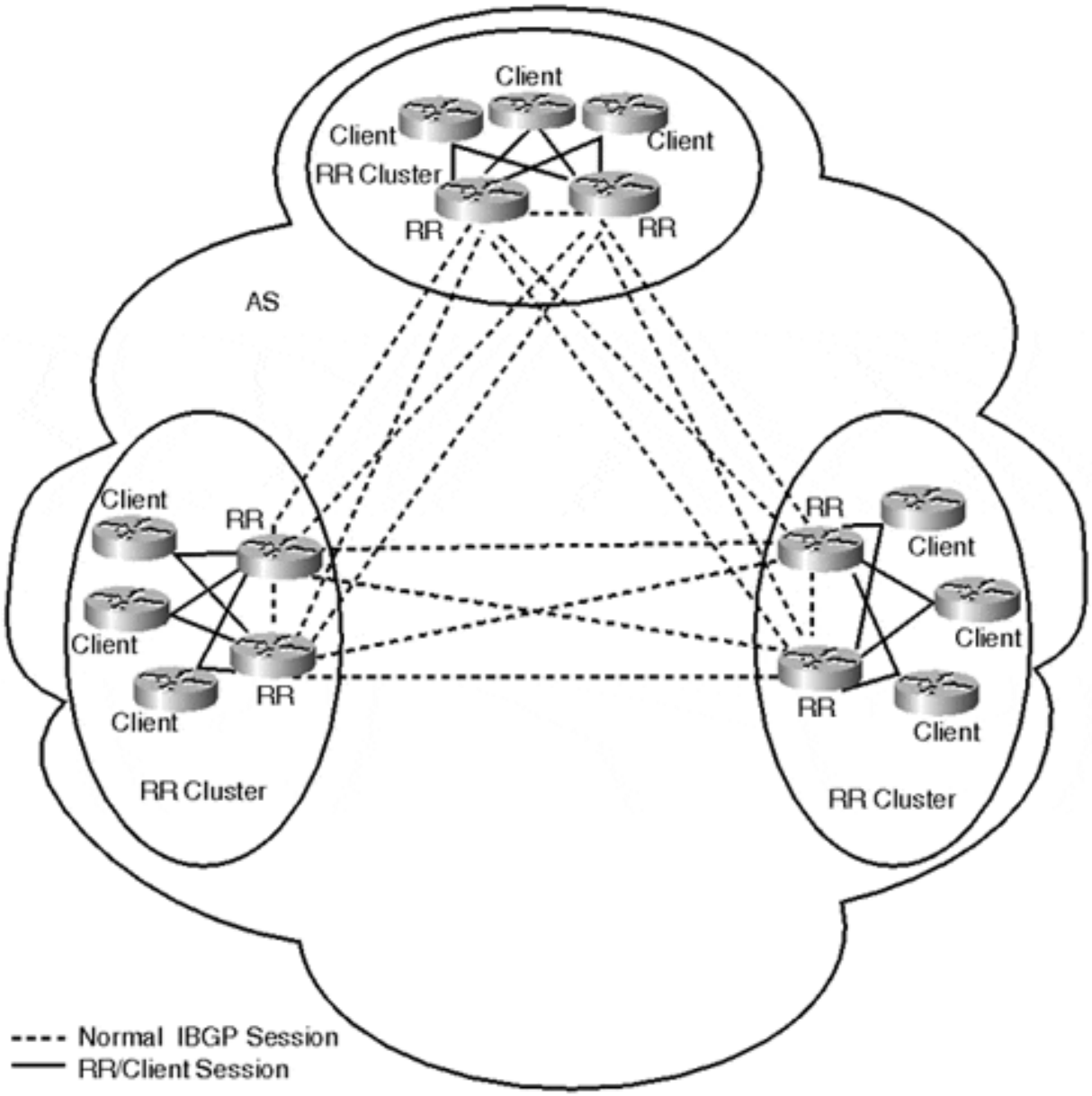

Рисунок 2.4 – Приклад мережі BGP з використанням відбивачів маршрутів

В результаті аналізу існуючих технологій та підходів до підвищення ефективності та надійності функціонування мережі BGP було вирішено впровадити методику відбивачів маршрутів.

Також для забезпечення більшої надійності мережі вирішено впровадити два відбивача маршрутів. Це дозволить уникнути перебоїв у роботі мережі в разі виходу з роботи одного з відбивачів маршрутів.

Для моделювання мережі було розглянуто два програмних продукти. Перший – Packet Tracer, розроблений корпорацією Cisco. Це емулятор мережі передачі даних, що випускається фірмою Cisco Systems. Дозволяє робити працездатні моделі мережі, налаштовувати (командами Cisco IOS) маршрутизатори і комутатори, взаємодіяти між декількома користувачами (через хмара). Включає в себе серії маршрутизаторів Cisco 1800, 2600, 2800 і комутаторів 2950, 2960, 3650. Крім того є сервери DHCP, HTTP, TFTP, FTP, робочі станції, різні модулі до комп'ютерів і маршрутизаторів, пристрої Wi-Fi, різні кабелі. Успішно дозволяє створювати навіть складні макети мереж, перевіряти на працездатність топології.

Cisco Packet Tracer – це потужна програма моделювання мережі, яка дозволяє студентам експериментувати з поведінкою мережі. Як невід'ємна частина Мережевих академій, Packet Tracer надає можливість моделювання, візуалізації, створення, оцінки, і можливості спільної роботи і полегшує викладання та вивчення складних понять різних технологій.

Packet Tracer розширює можливості фізичного обладнання в класі, дозволяючи студентам створювати мережі з практично необмеженою кількістю пристроїв, сприяє заохоченню практики, виявленню і усуненню неполадок. На основі моделювання умов навчання допомагає студентам розвивати навички 21 століття, такі як прийняття рішень, творчого та критичного мислення та вирішення проблем.

Packet Tracer доповнює програму Мережевих академій, дозволяючи інструкторам легко навчати і демонструвати складні технічні концепції і

проектування мережевих систем. Програмне забезпечення доступне безкоштовно для всіх інструкторів Мережевих академій, студентів і випускників.

Другим програмним продуктом є емулятор обладнання Cisco Dynamips. Dynamips є емулятором мережевого обладнання, який був написаний Крістофом Фіо. Dynamips працює на Linux, Mac OS X або Windows, і може емулювати апаратні серії платформ маршрутизації Cisco безпосередньо завантажуючи фактичне програмне забезпечення Cisco IOS в емулятор. Він дозволяє користувачам створювати складні мережеві топології для тестування функціональності IOS на настільному ПК, без необхідності реального фізичного пристрою Cisco. Dynamips в даний час підтримує різні середовища мереж, таких як Ethernet, послідовний порт, ATM, POS та інтерфейси апаратних платформ серій 1700, 2600, 3600, 3700, 7200.

Розвиток Dynamips зупинився на версії 0.2.8-RC2, випущеної в жовтні 2007 року. Є кілька додатків написаних для нього. Один з найбільш популярних є Dynagen, який реалізує інтерфейсні адд-они, які дозволяють використовувати INI-файл конфігурації для надання конфігурації мережі емулятору Dynamips. Іншим популярним додаткам є GNS3, що надає графічний інтерфейс для Dynamips і Dynagen. Вихідний код розповсюджується під ліцензією GNU GPL.

Остання модифікація Dynamips (з упором на зворотній інжиніринг) під назвою Dynamips-GDB була представлена в 2011 році і характеризується наявністю GDB заглушки, що доволило отримати прямий доступ до регістрів процесора і пам'яті віртуальної машини. Ця модифікація дозволяє проводити дебаг емулятора у будь-якому дебаггері, що підтримує протокол GDB, наприклад GNU Debugger, IDA Pro, Binnavi.

Було протестовано обидва програмних продукти і вирішено використовувати емулятор Dynamips, тому що він характеризується значно більшою кількістю підтримуваного обладнання, більшою продуктивністю та розширеним функціоналом, у порівнянні з Cisco Packet Tracer.

Модель мережі у емуляторі Dynamips зображена на рисунку 2.5.

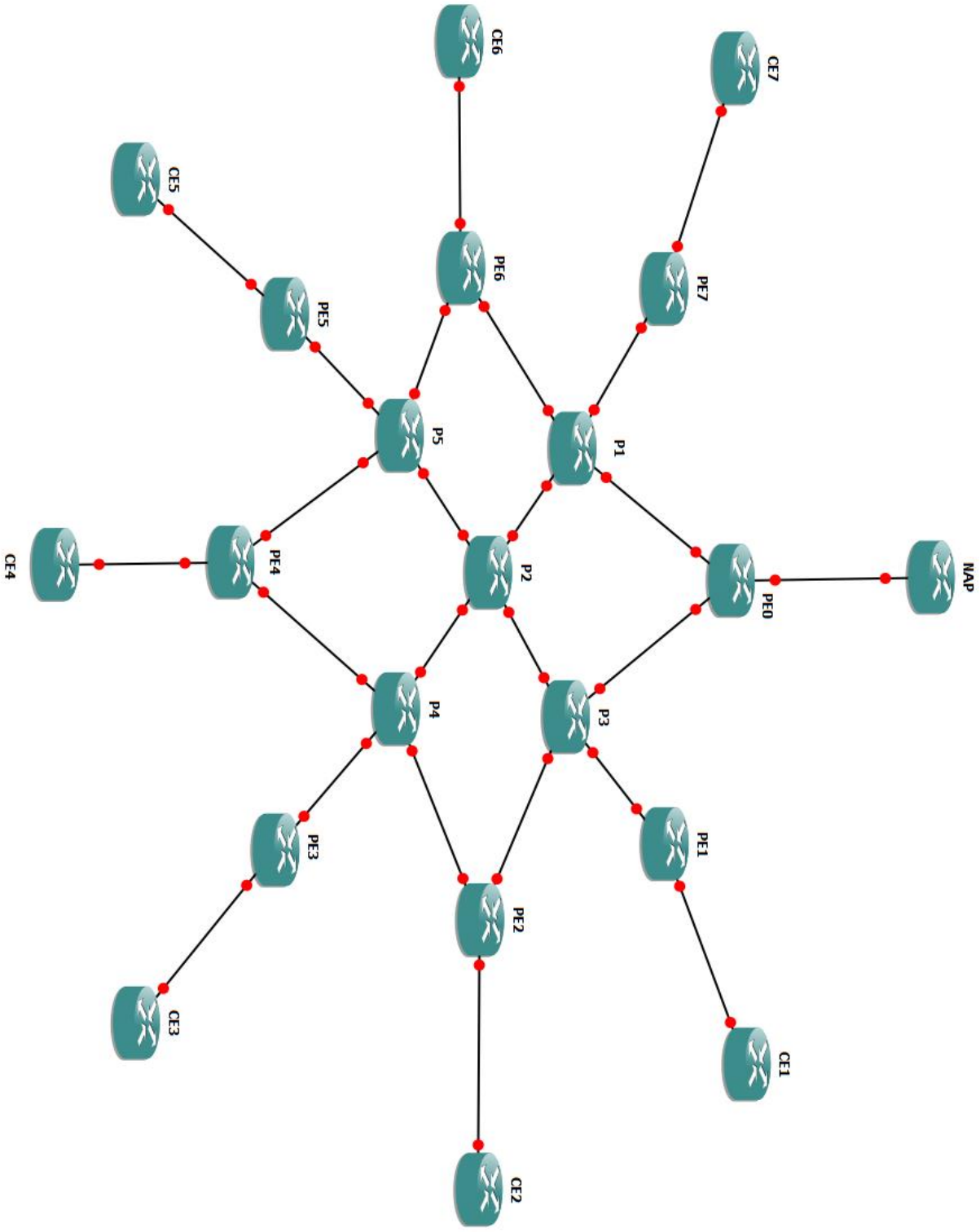

Рисунок 2.5 – Модель спроектованої мережі у емуляторі GNS3

Для взаємного підключення маршрутизаторів мережі було розрахованого маски підмереж для всіх з'єднань у мережі та для підмереж департаментів, див. рисунок 2.6.

Для обміну інформацією маршрутизації між кінцевими маршрутизаторами мережі MPLS та маршрутизаторами департаментів треба обрати один з протоколів маршрутизації внутрішнього шлюзу.

В результаті аналізу протоколів, описаних в розділі 1.3 було вирішено використати протокол OSPF. На маршрутизаторах департаментів та кінцевих маршрутизаторах мережі MPLS було сконфігуровано протокол OSPF в зоні 0, див. рисунок 2.7.

Також важливим моментом є розповсюдження інформації маршрутизації з департаментів у ядро мережі. Це було зроблено за допомогою можливостей операційної системи Cisco Interconnect Operating System.

Для моделювання було обрано обладнання корпорації Cisco Inc. Маршрутизатори MPLS мережі були спроектовані на основі моделі Cisco 7200, а маршрутизатори департаментів на основі Cisco 3660.

На рисунку 2.8 зображено модель мережі з зазначенням проколів маршрутизації.

Однією з завдань даної роботи є висока надійність та конфіденційність даних, що транспортуються по мережі. Для задоволення цієї умови, було вирішено кожен департамент підприємства виділити у окрему віртуальну приватну мережу (VPN).

Даний підхід дозволив повністю контролювати шляхи розповсюдження трафіку в розрізі окремих департаментів, тобто якщо корпоративна політика дозволяє обмін трафіки тільки між зазначеними департаментами, то всі інші варіанти розповсюдження будуть заборонені. Це досягається конфігурування окремої таблиці Virtual Roting/Forwarding для кожного департаменту.

Інформація маршрутизації кожного окремого департаменту абсолютно ізольована від інформації маршрутизації всіх інших департаментів підприємства.

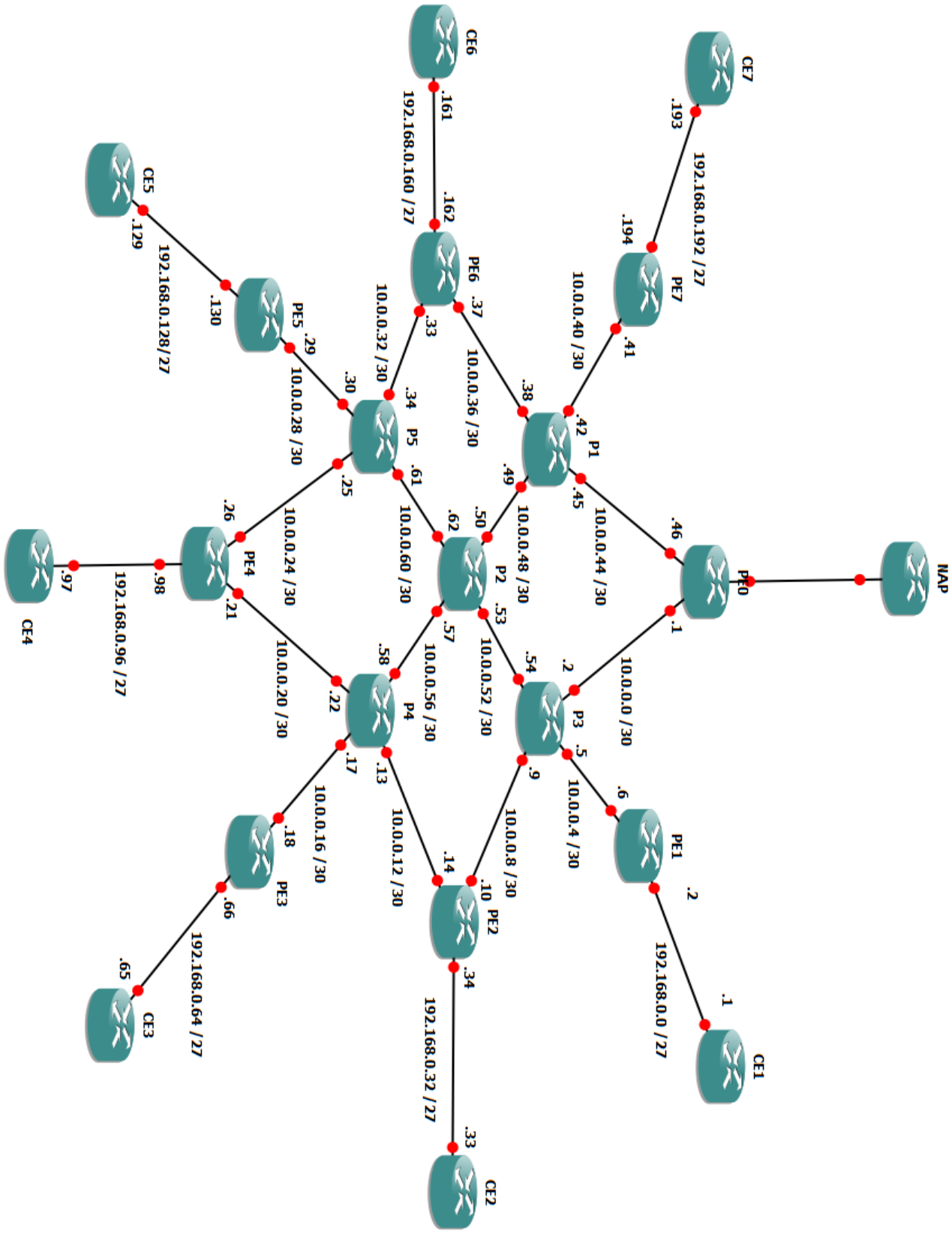

Рисунок 2.6 – Модель розробленої мережі з зазначенням адресації

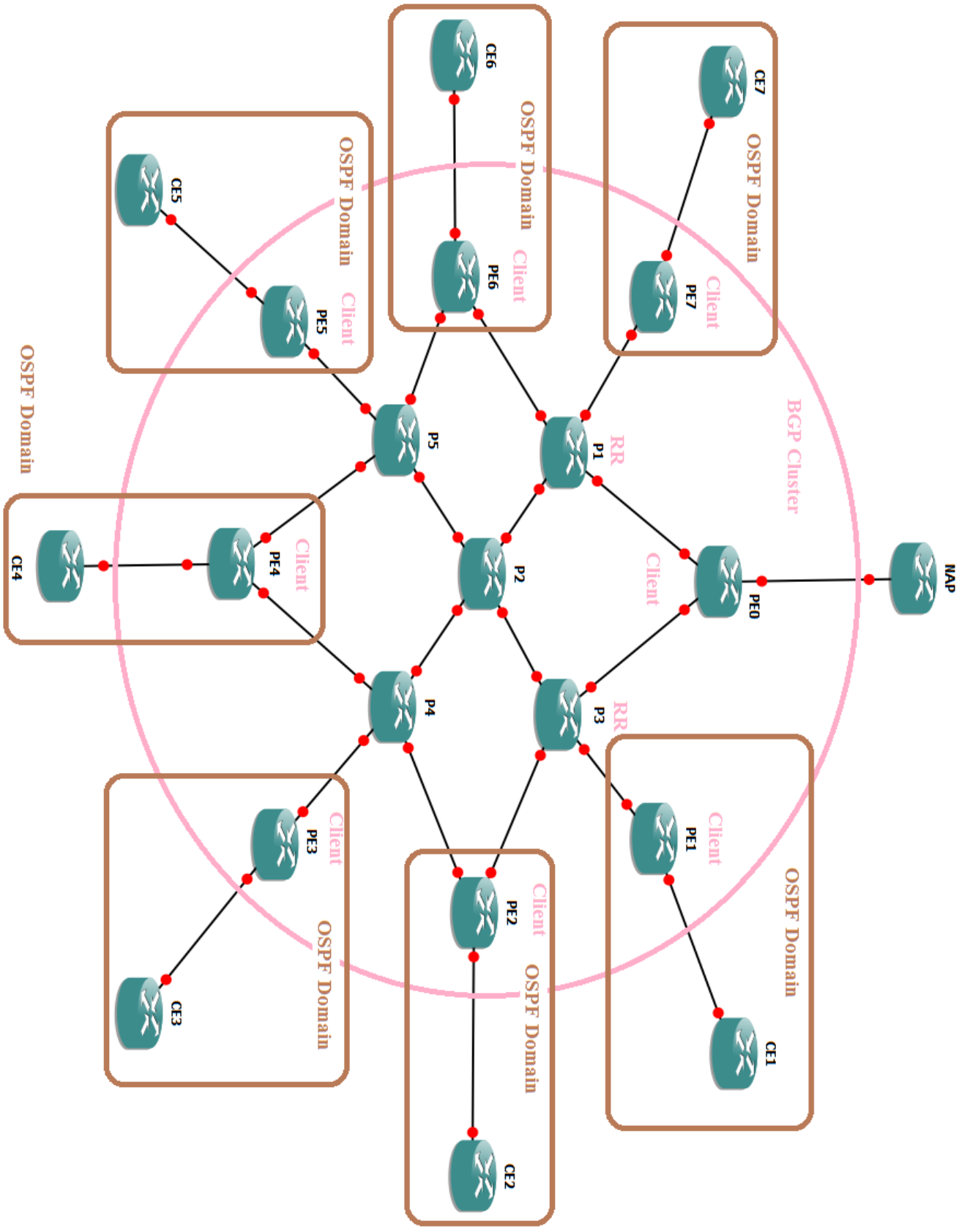

Рисунок 2.7 – Модель спроектованої мережі з зазначенням протоколів маршрутизації

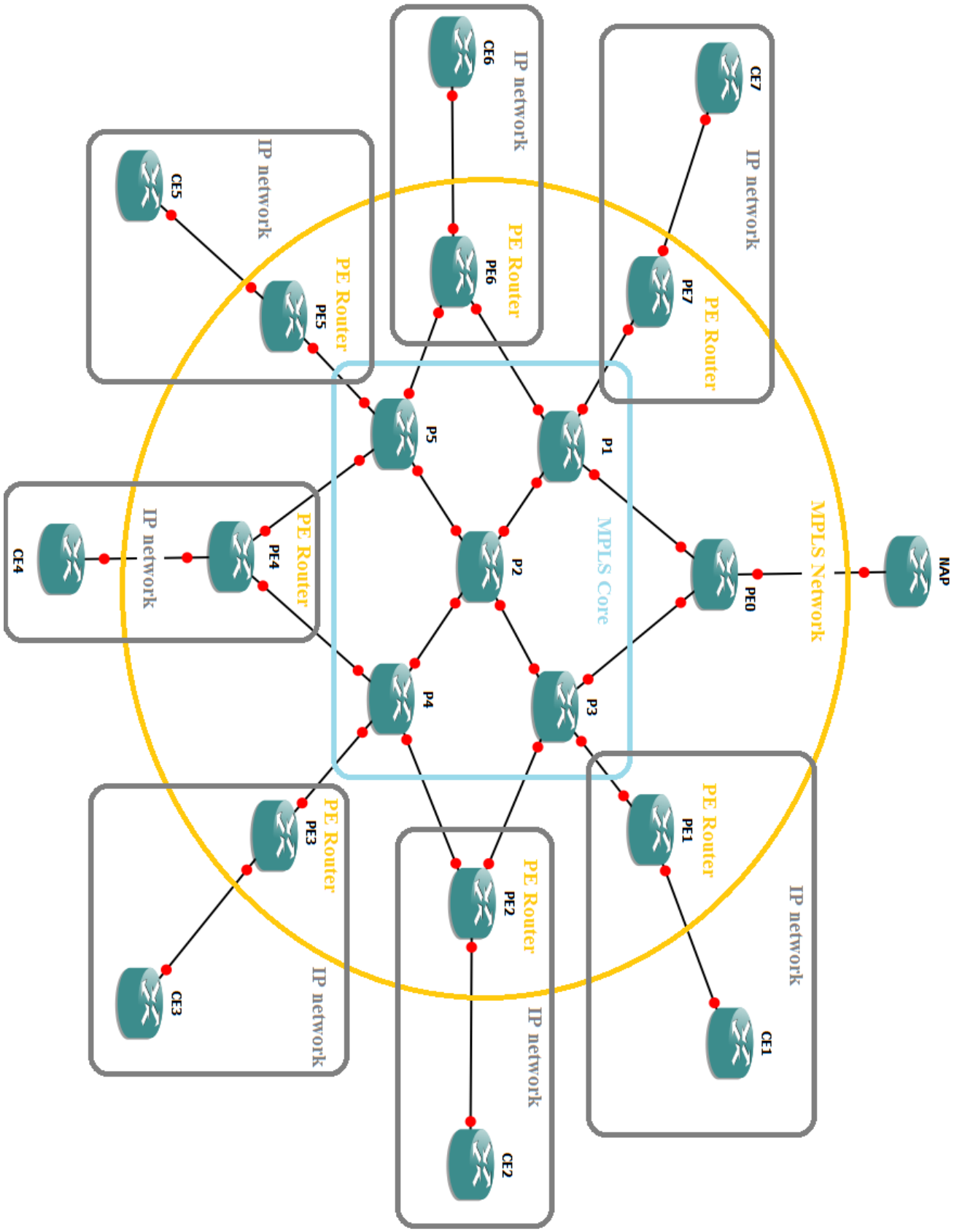

Рисунок 2.8 – Модель спроектованої мережі з зазначенням маршрутизуючих протоколів

Експорт, імпорт та об’єднання такої інформації регулюється на кінцевих маршрутизаторах мережі MPLS і підпорядковуються корпоративним політикам.

На рисунку 2.9 зображено модель спроектованої мережі з зазначенням віртуальних приватних мереже та таблиць VRF.

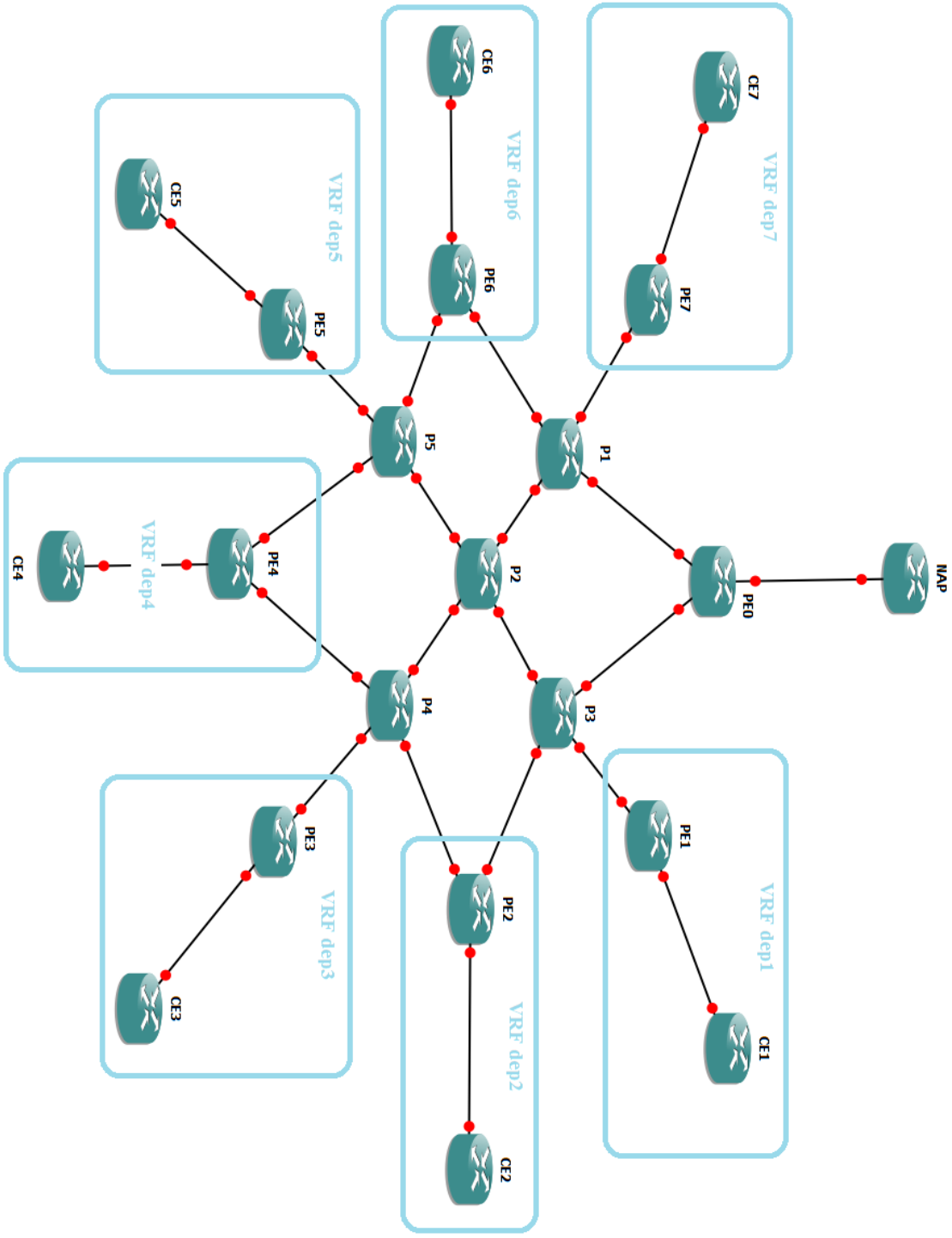

Рисунок 2.9 – Модель мережі з зазначенням таблиць VRF для віртуальних приватних мереж департаментів

3 РЕАЛІЗАЦІЯ МОДЕЛІ КОРПОРАТИВНОЇ МЕРЕЖІ

Модель спроектованої мережі було реалізовано у емуляторі Dynamips з використанням графічної оболонки GNS3. Головне вікно програми зображено на рисунку 3.1.

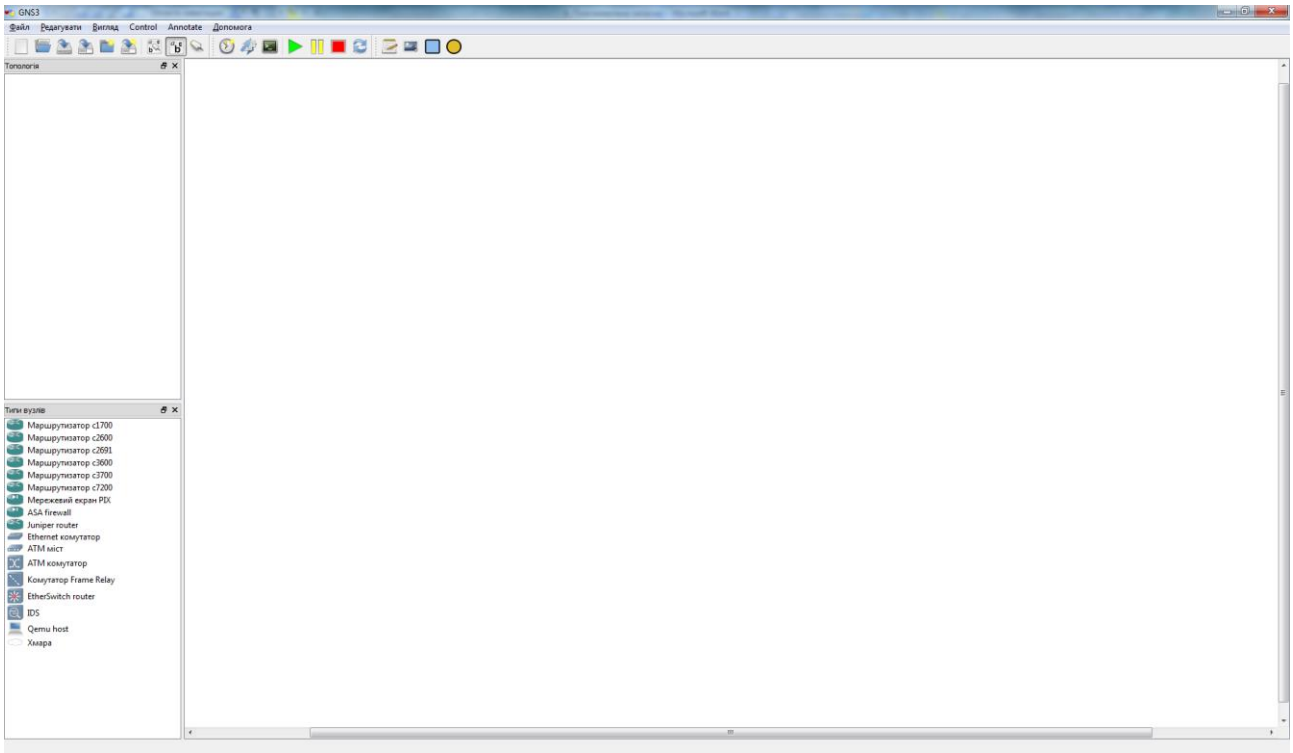

Рисунок 3.1 – Головне вікно емулятора GNS3

Даний емулятор підтримує широкий вибір мережевого обладнання Cisco, а саме:

- Маршрутизатори Cisco серії 1700: 1710, 1720, 1721, 1750, 1751, 1760
- Маршрутизатори Cisco серії 2600: 2610, 2611, 2610XM, 2620, 2620XM and 2650XM, 2611XM, 2621, 2621XM and 2651XM
- Маршрутизатори Cisco серії 3600: 3620, 3640, 3660
- Маршрутизатори Cisco серії 3700: 3725, 3745
- Маршрутизатори Cisco серії 7200: 7206
- Комутатори Cisco Catalyst
- Брандмауери Cisco PIX
- Брандмауери Cisco ASA

- Сенсори Cisco IDS
- Маршрутизатори Juniper

Вікно вибору обладнання у емуляторі Dynamips зображено на рисунку 3.2.

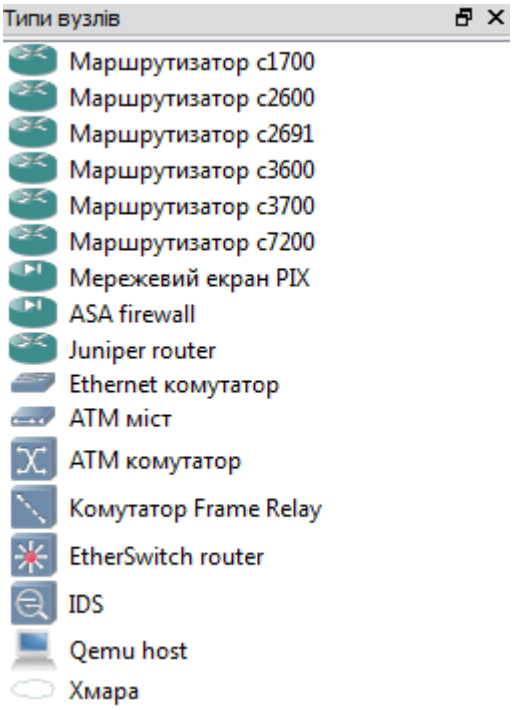

Рисунок 3.2

На рисунку 3.3 зображено вікно списку мережевого обладнання, яке входить в топологію проекту, а також перелічено мережеві інтерфейси кожного пристрою.

Нижче наведено конфігурації декількох маршрутизаторів, що сходять в реалізацію спроектованої моделі мережі.

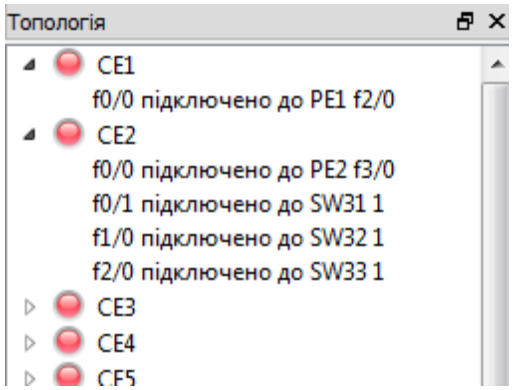

Рисунок 3.4 – Список обладнання, що входить в фізичну топологію проекта

Конфігурація маршрутизатора ядра мережі:

```
!
upgrade fpd auto
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P3
!
ip cef
no ipv6 cef
redundancy
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 ip address 10.0.0.54 255.255.255.252
 negotiation auto
 mpls ip
!
interface GigabitEthernet2/0
 ip address 10.0.0.5 255.255.255.252
 negotiation auto
 mpls ip
!
interface GigabitEthernet3/0
```

```
 ip address 10.0.0.9 255.255.255.252
 negotiation auto
 mpls ip
!
interface GigabitEthernet4/0
 ip address 10.0.0.2 255.255.255.252
 negotiation auto
 mpls ip
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
```

Конфігурація кінцевого маршрутизатора мережі MPLS:

```
!
hostname PE1
!
ip source-route
ip cef
!
ip vrf dep1
 rd 65000:1
 route-target export 65000:1
 route-target import 65000:1
```

```
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
redundancy
!
interface Loopback0
 ip address 10.0.0.101 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 ip address 10.0.0.6 255.255.255.252
 negotiation auto
 mpls ip
!
interface FastEthernet2/0
 ip vrf forwarding dep1
 ip address 192.168.0.2 255.255.255.224
 ip ospf 1 area 0
 duplex auto
 speed auto
!
interface FastEthernet2/1
 no ip address
 shutdown
```

```
 duplex auto
 speed auto
!
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
 !
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
router ospf 1 vrf dep1
 router-id 10.0.0.101
 log-adjacency-changes
 redistribute bgp 65000 subnets
!
router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.111 remote-as 65000
 neighbor 10.0.0.111 update-source Loopback0
 neighbor 10.0.0.112 remote-as 65000
 neighbor 10.0.0.112 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 10.0.0.111 activate
```

```
 neighbor 10.0.0.111 send-community extended
 neighbor 10.0.0.112 activate
 neighbor 10.0.0.112 send-community extended
exit-address-family
!
address-family ipv4 vrf dep1
 no synchronization
 redistribute ospf 1 vrf dep1
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
```

Нижче приведено частину конфігурації «відбивача маршрутів»:

```
!
router bgp 65000
 no synchronization
 bgp cluster-id 1
```

```
bgp log-neighbor-changes
neighbor 10.0.0.101 remote-as 65000
neighbor 10.0.0.101 update-source Loopback0
neighbor 10.0.0.101 route-reflector-client
neighbor 10.0.0.102 remote-as 65000
neighbor 10.0.0.102 update-source Loopback0
neighbor 10.0.0.102 route-reflector-client
neighbor 10.0.0.103 remote-as 65000
neighbor 10.0.0.103 update-source Loopback0
neighbor 10.0.0.103 route-reflector-client
neighbor 10.0.0.104 remote-as 65000
neighbor 10.0.0.104 update-source Loopback0
neighbor 10.0.0.104 route-reflector-client
neighbor 10.0.0.105 remote-as 65000
neighbor 10.0.0.105 update-source Loopback0
neighbor 10.0.0.105 route-reflector-client
neighbor 10.0.0.106 remote-as 65000
neighbor 10.0.0.106 update-source Loopback0
neighbor 10.0.0.106 route-reflector-client
neighbor 10.0.0.107 remote-as 65000
neighbor 10.0.0.107 update-source Loopback0
neighbor 10.0.0.107 route-reflector-client
neighbor 10.0.0.112 remote-as 65000
neighbor 10.0.0.112 update-source Loopback0
no auto-summary
!
address-family vpnv4
 neighbor 10.0.0.101 activate
 neighbor 10.0.0.101 send-community extended
 neighbor 10.0.0.102 activate
```

```
 neighbor 10.0.0.102 send-community extended
 neighbor 10.0.0.103 activate
 neighbor 10.0.0.103 send-community extended
 neighbor 10.0.0.104 activate
 neighbor 10.0.0.104 send-community extended
 neighbor 10.0.0.105 activate
 neighbor 10.0.0.105 send-community extended
 neighbor 10.0.0.106 activate
 neighbor 10.0.0.106 send-community extended
 neighbor 10.0.0.107 activate
 neighbor 10.0.0.107 send-community extended
 neighbor 10.0.0.112 activate
 neighbor 10.0.0.112 send-community extended
exit-address-family
!
```

ВИСНОВКИ

В даному дипломному проекті було спроектовано інформаційно-обчислювальну мережу корпоративного масштабу на базі технології MPLS. В процесі розробки було розглянуто та проаналізовано найновіші та найбільш вживані технології та протоколи, що використовуються у мережах зазначеного масштабу.

В побудованій мережі використані такі технології та протоколи, як Open Shortest Path First, Internet Protocol, Multiprotocol Label Switching, Border Gateway Protocol with Multiprotocol Extensions та інші.

Також в розробленій мережі використано технологію MPLS Virtual Private Network, що дає змогу дуже гнучко регулювати можливість обміну трафіку між департаментами підприємства.

В результаті виконання дипломного проекту було отримано корпоративну мережу, яка характеризується високими параметрами захищеності, конфіденційності інформації та відмовостійкості. Слід особливо відмітити, що завдяки набору використаних технологій, дана мережа також відповідає високим вимогам до масштабованості мережі, як в плані розширення або зменшення ядра мережі, так і з точки зору зміни кількості департаментів підприємства.

Щодо перспектив розвитку та шляхів подальшого покращення даної мережі можна відмитити можливість впровадження таких технологій, як Dynamic Multipoint Virtual Private Network та MPLS VPN with Common Services, що дасть змогу підвищити захищеність мережі шляхом шифрації транспортованого трафіку та підвищити легкість конфігурування та розділення послуг, що надаються окремим департаментам підприємства.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Павлов О.А. Інформаційні технології та алгоритмізація в управлінні [Текст] / О.А.Павлов, С.Ф.Теленик. — К.: Техніка, 2002. — 344 с.
2. Теленик С.Ф. Управління центрами оброблення даних [Текст] / С.Ф.Теленик, О.І.Ролік, М.М.Букасов, К.О.Крижова // Вісн. Львів. ун-ту. Сер. прикл. матем. інформатики.— 2009.— Вип. 11.— С.87—99.
3. Теленик С. Управління ресурсами і навантаженням інформаційно-телекомунікаційних систем [Текст] / С. Теленик, О. Ролік, М. Букасов // Вісн. Тернопільського держ. техн. ун-ту. — 2009.— Вип.4.— С.106—119.
4. Number of employees at Cisco by geographic region from 2010 to 2018 [Електронний ресурс]. – Режим доступу: https://www.statista.com/statistics/350519/cisco-employees-by-region/. – 12.02.2019.
5. Snevely R. Enterprise Data Center Design and Methodology / R. Snevely. – Sun Microsystems Press. – 2006. – 220 p.
6. Кученко Ю. ЦОД как объект системной и структурной оптимизации / Ю. Кученко // Компьютерное обозрение – 2009. – №15.
7. Schulz G. The Green and Virtual Data Center / G. Schulz // CRC Press, Taylor & Francis Group. – 2009. – 376 p.
8. Теленик С.Ф. Моделі управління розподілом обмежених ресурсів в інформаційно-телекомунікаційній мережі / С.Ф. Теленик, О.І. Ролік, М.М. Букасов // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка. – К.: Екотех. — 2006.— №44.— С. 243—246.
9. Urgaonkar B. Resource overbooking and application profiling in shared hosting platforms / B. Urgaonkar, P. Shenoy, and T. Roscoe // in Proc. Fifth Symposium on Operating Systems Design and Implementation, Boston, MA, Dec. 2002.
10. Aron M. Cluster reserves: A mechanism for resource management in cluster-based network servers / M. Aron, P. Druschel, and W. Zwaenpoel // in Proc. ACM SIGMETRICS, Santa Clara, CA, Jun. 2000.

11. Wolf J.L. Disk load balancing for video-on-demand systems / J. L.Wolf, P. S. Yu, and H. Shachinai // ACM/Springer Multimedia Systems Journal. – Vol. 5(6). – 1997. – pp. 358–370.

12. FEDERGRUEN, A. The greedy procedure for resource allocation problems: Necessary and sufficient conditions for optimality / A. FEDERGRUEN, H. GROENVELT // Oper. Res., Vol. 34. – 1986. – pp. 908–918.

13. Kellerer H. Knapsack Problems / H. Kellerer, U. Pferschy and D. Pisinger // Springer, 2004.

14. Shachnai H. On two class-constrained versions of the multiple knapsack problem / H. Shachnai and T. Tamir // Algorithmica, Vol. 29 (2001). – pp. 442–467.

15. Chase J. Managing Energy and Server Resources in Hosting Centers / J. Chase and etc. // In Proceedings of the Eighteenth ACM Symposium on Operating Systems Principles (SOSP). – October 2001. – pp. 103–116.

16. Cherkasova L. Computer Systems and Technology Laboratory - HP Laboratories Palo Alto - FLEX: Design and Management Strategy for Scalable Web Hosting Service / L. Cherkasova // HPL-1999-64(R.1) October, 1999.